Symantec™ Endpoint Protection 14.2.1 Installation and Administration Guide

Symantec Endpoint Protection Installation and Administration Guide

Product version 14.2.1 (14.2 RU1)

Documentation version: 1

This document was last updated on: April 23, 2019

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Symantec Support

Knowledge Base articles and Symantec Connect

Before you contact Technical Support, you can find free content in our online Knowledge Base, which includes troubleshooting articles, how-to articles, alerts, and product manuals. In the search box of the following URL, type the name of your product:

https://support.symantec.com/

Access our blogs and online forums to engage with other customers, partners, and Symantec employees on a wide range of topics at the following URL:

https://www.symantec.com/connect/

Technical Support and Enterprise Customer Support

Symantec Support maintains support centers globally 24 hours a day, 7 days a week. Technical Support's primary role is to respond to specific queries about product features and functionality. Enterprise Customer Support assists with non-technical questions, such as license activation, software version upgrades, product access, and renewals.

Before you contact Symantec Support, see:

https://entced.symantec.com/default/ent/supportref

To contact Symantec Support, see:

https://support.symantec.com/en_US/contact-support.html

Contents

Chapter 1

Introduction to Symantec Endpoint Protection

This chapter includes the following topics:

What is Symantec Endpoint Protection?

Symantec Endpoint Protection is a client-server solution that protects laptops, desktops, and servers in your network against malware, risks, and vulnerabilities. Symantec Endpoint Protection combines virus protection with advanced threat protection to proactively secure your client computers against known and unknown threats, such as viruses, worms, Trojan horses, and adware. Symantec Endpoint Protection 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 both physical systems and virtual systems against attacks. Symantec Endpoint Protection provides management solutions that are efficient and easy to deploy and use.

See “How Symantec Endpoint Protection technologies protect your computers” on page 28.

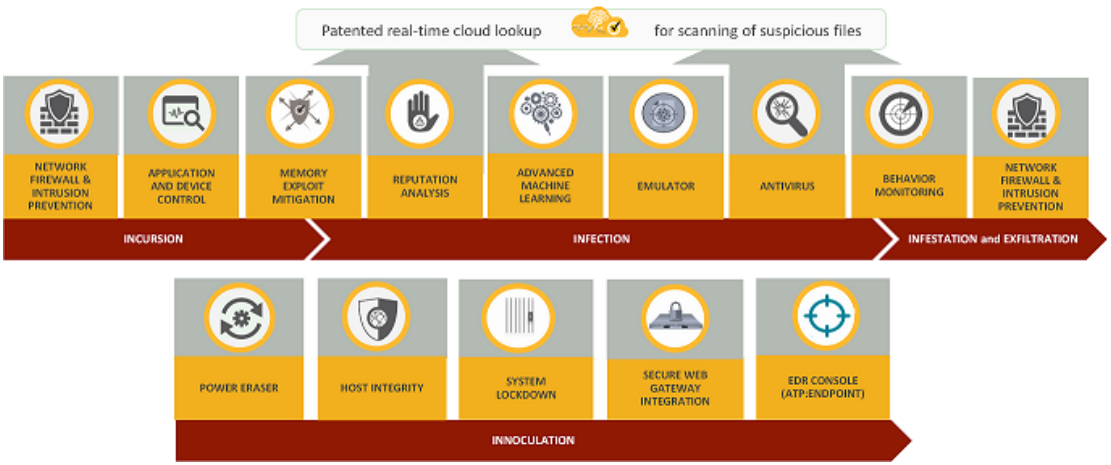
See “Symantec Endpoint Protection architecture components” on page 31.

How Symantec Endpoint Protection technologies protect your computers

Symantec Endpoint Protection's core protection against known and unknown threats uses a layered approach to defense. The comprehensive approach protects the network before, during, and after an attack. Symantec Endpoint Protection reduces your risk of exposure by providing tools to increase your security posture ahead of any attack.

To get complete protection for the computers in your network, enable all protections at all times.

Figure 1-1 How Symantec Endpoint Protection stops targeted attacks and zero-day threats with layered protection



What types of attacks do Symantec Endpoint Protection technologies protect against?

Symantec Endpoint Protection uses the following holistic security approach to protect your environment across the entire attack chain, using the following stages: incursion, infection, infestation and exfiltration, and remediation and inoculation.

Phase 1: Incursion

During the incursion phase, hackers typically break into the organization's network using target attacks such as social engineering, zero-day vulnerabilities, SQL injection, targeted malware, or other methods.

Symantec Endpoint Protection protects against attacks before they enter your system using the following technologies:

- **Intrusion Prevention/Firewall (Network Threat Protection)**: Analyzes all incoming traffic and outgoing traffic and offers browser protection to block such threats before they can be

executed on the computer. The rules-based firewall and browser protection protect against web-based attacks.

See "Managing intrusion prevention" on page 377.
See "Managing firewall protection" on page 336.

- **Application Control**: Controls the file access and registry access and how processes are allowed to run.

  See "About application control, system lockdown, and device control" on page 502.
  See "Setting up application control" on page 503.

- **Device Control**: Restricts the access to select hardware and control what types of devices can upload or download information.

  See "Managing device control" on page 538.

- **Memory Exploit Mitigation**: Neutralizes zero-day exploits like Heap Spray, SEHOP overwrite, and Java exploits in popular software that the vendor has not patched.

  See "Hardening Windows clients against memory tampering attacks with a Memory Exploit Mitigation policy" on page 393.

Phase 2: Infection

In targeted attacks, hackers typically break into the organization's network using social engineering, zero-day vulnerabilities, SQL injection, targeted malware, or other methods.

Symantec Endpoint Protection uses the following technologies to detect and prevent these attacks before they infect your system:

- **Memory Exploit Mitigation**: Detects malware.
- **File reputation analysis (Insight)**: Based on the artificial intelligence that uses Symantec's global intelligence network. This advanced analysis examines billions of correlated linkages from users, websites, and files to identify and defend against rapidly-mutating malware. By analyzing key attributes (such as the origin point of a file download), Symantec can accurately identify whether a file is good or bad and assign a reputation score all before the file arrives on the client computer.

  See "Managing Download Insight detections" on page 442.

- **Advanced machine learning**: Analyzes the trillions of examples of the good files and bad files that are contained in a global intelligence network. Advanced machine learning is a signatureless technology that can block new malware variants at the pre-execution.

  See "How does Symantec Endpoint Protection use advanced machine learning?" on page 447.

- **High-speed emulation**: Detects hidden malware using polymorphic custom packers. A scanner runs each file in milliseconds in a lightweight virtual machine that causes threats to reveal themselves, improving both the detection rates and performance.

  See "How does the emulator in Symantec Endpoint Protection detect and clean malware?" on page 450.

- **Antivirus file protection (Virus and Spyware Protection)**: Uses signature-based antivirus and file heuristics to look for and eradicate malware on a system to protect against viruses, worms, Trojans, spyware, bots, adware, and rootkits.
  See "Managing scans on client computers" on page 415.
  See "About the types of scans and real-time protection" on page 418.
- **Behavioral monitoring (SONAR)**: Leverages machine learning to provide zero-day protection, stopping new and unknown threats by monitoring nearly 1,400 file behaviors while they execute in real time to determine file risk.
  See "Managing SONAR" on page 495.

Phase 3: Infestation and Exfiltration

Data exfiltration is the unauthorized transfer of data from a computer. Once the intruders control these target systems, they may steal intellectual property or other confidential data. Attackers use captured information for analysis and further exploitation or fraud.

- **Intrusion Prevention/Firewall**: Block threats as they travel through the network.
- **Behavioral monitoring**: Helps stop the spread of infection.

Phase 4: Remediation and Inoculation

Symantec Endpoint Protection includes a single console and agent that offers protection across operating systems, platforms, and businesses of any size.

- **Power Eraser**: An aggressive tool, which can be triggered remotely, to address advanced persistent threats and remedy tenacious malware.
  See "What you should know before you run Power Eraser from the Symantec Endpoint Protection Manager console" on page 781.
- **Host Integrity**: Ensures that endpoints are protected and compliant by enforcing policies, detecting unauthorized changes, and conducting damage assessments. Host Integrity then isolates a managed system that does not meet your requirements.
  See "How Host Integrity works" on page 605.
- **System Lockdown**: Allows the whitelisted applications (known to be good) to run, or blocks the blacklisted applications (known to be bad) from running. In either mode, System Lockdown uses checksum and file location parameters to verify whether an application is approved or unapproved. System Lockdown is useful for kiosks where you want to run a single application only.
  See "Configuring system lockdown" on page 516.
- **Secure Web Gateway Integration**: Uses programmable REST APIs to make integration possible with Secure Web Gateway, to help quickly stop the spread of infection at the client computer.
- **EDR Console Integration**. Symantec Endpoint Protection is integrated with Symantec Endpoint Detection and Response and is designed to detect, respond, and block targeted

attacks and advanced persistent threats faster by prioritizing attacks. EDR (Endpoint Detection and Response) capability is built into Symantec Endpoint Protection, which makes it unnecessary to deploy additional agents.

See "Configuring system lockdown" on page 516.

What types of attacks do Symantec Endpoint Protection technologies protect against?

Table 1-1 displays which types of Symantec Endpoint Protection technologies protects against which types of attacks.

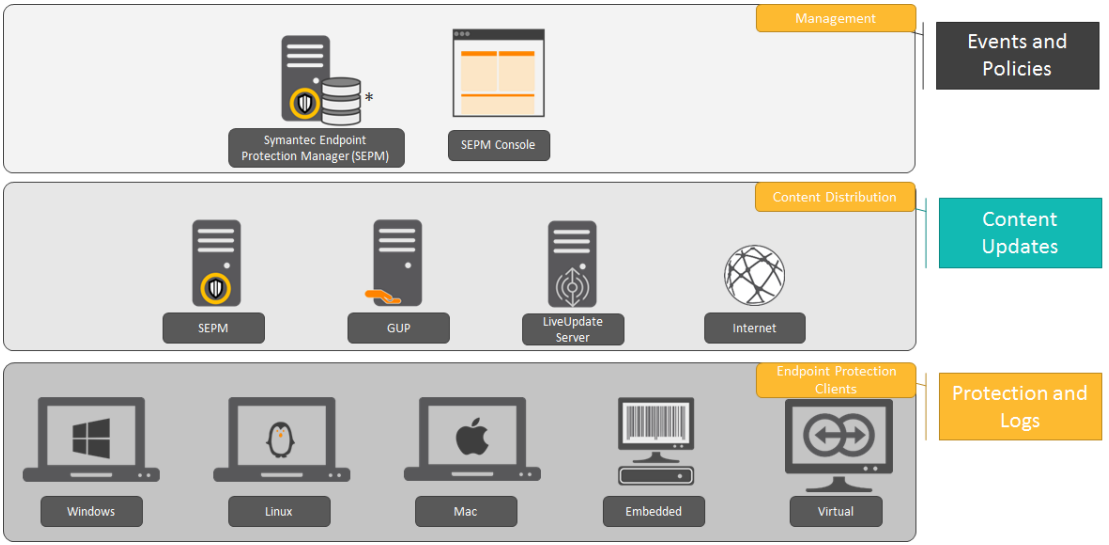
Table 1-1 What types of attacks does each Symantec Endpoint Protection technology protect against?

Attack	Advanced machine learning	Heuristics	Intrusion Prevention	Network Protection	Policy lockdown
Zero-day	√	√	√		√
Social engineering	√	√	√	√	√
Ransomware	√	√		√	√
Targeted attack	√	√	√		√
Advanced persistent threat	√	√	√		
Drive-by download		√	√		

Symantec Endpoint Protection architecture components

The Symantec Endpoint Protection architecture uses three functional groups of components. Some of the components belong in multiple groups because they are multi-functional.

Figure 1-2 Symantec Endpoint Protection components



* Symantec Endpoint Protection Manager can use an embedded database or Microsoft SQL Server.

Main product components

Table 1-2 Main components

Component	Description
Symantec Endpoint Protection Manager	Symantec Endpoint Protection Manager is a management server that manages events, policies, and client registration for the client computers that connect to your company's network. Symantec Endpoint Protection Manager includes the following subcomponents: ■ 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. ■ The embedded database stores security policies and events and is installed with Symantec Endpoint Protection Manager. You can also install a SQL Server database to use instead of the embedded database. SQL Server is recommended for larger organization 1000+ computers. See "Installing Symantec Endpoint Protection Manager" on page 43.
Symantec Endpoint Protection client	The Symantec Endpoint Protection client provides the security protection part of the solution. The client downloads policies and sometimes content from the Symantec Endpoint Protection Manager and runs on Windows, Mac, and Linux.

See "What is Symantec Endpoint Protection?" on page 27.

Optional product components

Symantec Endpoint Protection enables a client to download content from the management server, Group Update Provider, an Internal LiveUpdate server, or the Internet.

Table 1-3 Optional components and their functions

Component	Description
LiveUpdate Administrator	LiveUpdate Administrator downloads definitions, signatures, and other content from an internal LiveUpdate server and distributes the updates to client computers. You can use an internal LiveUpdate server in very large networks to reduce the load on the Symantec Endpoint Protection Manager. You should also use the internal LiveUpdate server if your organization runs multiple Symantec products that also use LiveUpdate to update client computers. You can get LiveUpdate Administrator from Download LiveUpdate Administrator (LUA). See "Choose a distribution method to update content on clients" on page 179. See "Configuring clients to download content from an internal LiveUpdate server" on page 196.
Group Update Provider (GUP)	The Group Update Provider helps distribute content within the organization, particularly useful for groups at remote locations with minimal bandwidth. Organizations that have a lot of clients may want to use Group Update Providers (GUPs) for Windows clients. 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 215.
Symantec Endpoint Protection cloud console	The cloud console provides cloud-based management that extends Symantec Endpoint Protection abilities to detect and remediate emerging threats in your environment. To use the cloud console, you must first enroll each Symantec Endpoint Protection Manager domain. See "Introduction to the Symantec Endpoint Protection 14.2 cloud console" on page 577. See "Enrolling a 14.1/14.2 domain in the cloud console from the Symantec Endpoint Protection Manager console" on page 578.

Symantec Endpoint Protection also comes with multiple tools to help you increase security and manage the product.

See "What are the tools included with Symantec Endpoint Protection?" on page 837.

See "How Symantec Endpoint Protection technologies protect your computers" on page 28.

Where to get more information

Table 1-4 displays the websites where you can get best practices, troubleshooting information, and other resources to help you use the product.

Table 1-4 Symantec website information

Types of information	Website link
Trial versions	Trialware (14.x)
Manuals and documentation updates	**English:** ■ Symantec Product Documentation ■ Product guides for all versions of Symantec Endpoint Protection 12.1.x ■ Product guides for all versions of Symantec Endpoint Protection 14.x **Other languages:** ■ Brazilian Portuguese ■ Chinese (simplified) ■ Chinese (traditional) ■ French ■ German ■ Italian ■ Japanese ■ Korean ■ Spanish *Czech, Polish, and Russian files are on the English page.
Technical Support	Endpoint Protection Technical Support Includes knowledge base articles, product release details, updates and patches, and contact options for support.
Threat information and updates	Symantec Security Center
Training	■ Symantec Education Services Access the training courses, the eLibrary, and more.
Symantec Connect forums	Endpoint Protection

Chapter 2

Getting Started with Symantec Endpoint Protection

This chapter includes the following topics:

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.

Perform the following tasks to install and protect the computers in your network immediately:

- Step 1: Plan your installation structure
- Step 2: Prepare for and then install Symantec Endpoint Protection Manager
- Step 3: Add groups, policies, and locations
- Step 4: Change communication settings to increase performance
- Step 5: Activate the product license
- Step 6: Decide on a client deployment method
- Step 7: Prepare the client for installation
- Step 8: Deploy and install the client software
- Step 9: Check that the computers are listed in the groups that you expected and that the clients communicate with the management server

See "What do I do after I install the management server?" on page 65.

Step 1: Plan your installation structure

Before you install the product, consider the size and geographical distribution of your network to determine the installation architecture.

To ensure good network and database performance, you need to evaluate several factors. These factors include how many computers need protection, whether any of those computers connect over a wide-area network, or how often to schedule content updates.

- If your network is small, is located in one geographic location, and has fewer than 500 clients, you need to install only one Symantec Endpoint Protection Manager.
- If the 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.
- If your network is geographically dispersed, you may need to install additional management servers for load balancing and bandwidth distribution purposes.

To help you plan medium to large-scale installations, see: Symantec Endpoint Protection Sizing and Scalability Best Practices White Paper.

See "Network architecture considerations" on page 84.

See "Setting up sites and replication" on page 739.

See "Setting up failover and load balancing" on page 732.

Step 2: Prepare for and then install Symantec Endpoint Protection Manager

1. Make sure the computer on which you install the management server meets the minimum system requirements.

   See: Release notes, new fixes, and system requirements for all versions of Endpoint Protection

2. To install Symantec Endpoint Protection Manager, you must be logged on with an account that grants local administrator access.

3. Decide on whether to install the embedded database or use a Microsoft SQL Server database.

   If you 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.

   See “About SQL Server configuration settings” on page 87.

   See “Setting up failover and load balancing” on page 732.

4. You install Symantec Endpoint Protection Manager first. After you install, you immediately configure the installation with the Management Server Configuration Wizard.

   Decide on the following items when you configure the management server:

   - A password for your logon 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

   See “Installing Symantec Endpoint Protection Manager” on page 43.

   See “About basic management server settings” on page 86.

   See “Configuring Symantec Endpoint Protection Manager after installation” on page 44.

Step 3: Add groups, policies, and locations

1. You use groups to organize the client computers, and apply a different level of security to each group. You can use the default groups, import groups if your network uses Active Directory or an LDAP server, or add new groups.

   If you add new groups, you can use the following group structure as a basis:

   - Desktops
   - Laptops

- Servers

See "Importing existing groups and computers from an Active Directory or an LDAP server" on page 237.

See "How you can structure groups" on page 236.

See "Adding a group" on page 237.

2. You use locations to apply different policies and settings to computers based on specific criteria. For example, you can apply different security policies to the computers based on whether they are inside or outside the company network. In general, the computers that connect to your network from outside of your firewall need stronger security than those that are inside your firewall.

   A location can allow the mobile computers that are not in the office to update their definitions automatically from Symantec's LiveUpdate servers.

   See Best Practices for Symantec Endpoint Protection Location Awareness.

   See "Adding a location to a group" on page 266.

3. Disable inheritance for the groups or locations for which you want to use different policies or settings.

   By default, groups inherit their policies and settings from the default parent group, **My Company**. If you want to assign a different policy to child groups, or want to add a location, you must first disable inheritance. Then you can change the policies for the child groups, or you can add a location.

   Note: Symantec Endpoint Protection Manager policy inheritance does not apply to the policies that are received from the cloud. The cloud policies follow the inheritance as defined in the cloud.

   See "Disabling a group's inheritance" on page 242.

4. For each type of policy, you can accept the default policies, or create and modify new policies to apply to each new group or location. You must add requirements to the default Host Integrity policy for the Host Integrity check to have an effect on the client computer.

Step 4: 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. 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

environments might need a longer heartbeat interval. Symantec recommends that you leave **Let clients upload critical events immediately** checked.

- 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 206.

See "Updating policies and content on the client using push mode or pull mode" on page 165.

Step 5: Activate the product license

Purchase and activate a license within 60 days of product installation.

See "Licensing Symantec Endpoint Protection" on page 94.

See "Symantec Endpoint Protection product license requirements" on page 80.

See "Activating or importing your Symantec Endpoint Protection product license" on page 51.

Step 6: Decide on a client deployment method

Determine which client deployment method would work best to install the client software on your computers in your environment.

See "Choosing a method to install the client using the Client Deployment Wizard" on page 119.

- For Linux clients, you can use either **Save Package** or **Web Link and Email**, but not **Remote Push**.
- For Windows and Mac clients, if you use **Remote Push**, you may need to do the following tasks:
  - Make sure that administrator access to remote client computers is available. Modify any existing firewall settings (including ports and protocols) to allow remote deployment between Symantec Endpoint Protection Manager and the client computers.
    See "Communication ports for Symantec Endpoint Protection" on page 112.
  - You must be logged on with an account that grants local administrator access.
    If the client computers are part of an Active Directory domain, you must be logged on to the computer that hosts Symantec Endpoint Protection Manager with an account that grants local administrator access to the client computers. You should have administrator credentials available for each client computer that is not part of an Active Directory domain.
    See "Preparing Windows and Mac computers for remote deployment" on page 108.

See "Preparing for client installation" on page 107.

Step 7: Prepare the client for installation

1. Make sure that the computers on which you install the client software meet the minimum system requirements. You should also install the client on the computer that hosts Symantec Endpoint Protection Manager.

   See: Release notes, new fixes, and system requirements for all versions of Endpoint Protection

2. Manually uninstall any third-party security software programs from Windows computers that the Symantec Endpoint Protection client installer cannot uninstall.

   For a list of products that this feature removes, see: Third-party security software removal support in Symantec Endpoint Protection

   You must uninstall any existing security software from Linux computers or from Mac computers.

   Some programs may have special uninstallation routines, or may need to have a self-protection component disabled. See the documentation for the third-party software.

3. As of 14, you can configure the installation package to remove a Windows Symantec Endpoint Protection client that does not uninstall through standard methods. When that process completes, it then installs Symantec Endpoint Protection.

   See "Configuring client packages to uninstall existing security software" on page 124.

Step 8: Deploy and install the client software

1. For Windows clients, do the following tasks:

   - Create a custom client install feature set that determines which components you install on the client computers. You can also use one of the default client install feature sets.
     See "Importing existing groups and computers from an Active Directory or an LDAP server" on page 237.
     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**.
   - Update custom client install settings to determine installation options on the client computer. These options include the target installation folder, the uninstallation of third-party security software, and the restart behavior after installation completes. You can also use the default client install settings.
     See "Choosing which security features to install on the client" on page 121.

2. With the Client Deployment Wizard, create a client installation package with selections from the available options, and then deploy it to your client computers. You can only deploy to Mac or Windows computers with the Client Deployment Wizard.

   See "Installing Symantec Endpoint Protection clients with Web Link and Email" on page 63.

See "Installing Symantec Endpoint Protection clients with Remote Push" on page 60.

See "Installing Symantec Endpoint Protection clients with Save Package" on page 53.

See "Exporting client installation packages" on page 136.

Symantec recommends that you do not perform third-party installations simultaneous to the installation of Symantec Endpoint Protection. The installation of any third-party programs that make network- or system-level changes may cause undesirable results when you install Symantec Endpoint Protection. If possible, restart the client computers before you install Symantec Endpoint Protection.

Step 9: 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 "Checking whether the client is connected to the management server and is protected" on page 163.
   - The **Last Time Status Changed** column displays the time that each client last communicated with the management server.
   - The **Restart Required** column displays whether or not the client computers need to be restarted to be protected.
     See "Restarting the client computers from Symantec Endpoint Protection Manager" on page 127.
   - 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 168.
     See "Updating client policies" on page 313.

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 client computers" on page 247.

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 767.

See "Checking whether the client is connected to the management server and is protected" on page 163.

See "Troubleshooting connectivity problems between Symantec Endpoint Protection Manager and the Symantec Endpoint Protection client" on page 765.

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.

For the most current system requirements, see: Release notes, new fixes, and system requirements for all versions of Endpoint Protection

Some Symantec products may cause conflicts with Symantec Endpoint Protection Manager when they are installed on the same server. For information about any necessary configuration changes in those products, see: Software compatibility with Symantec Endpoint Protection

In addition, Symantec Endpoint Protection Manager installation and configuration checks the security policies for the required rights to allow the virtual service accounts to run correctly. Symantec Endpoint Protection Manager automatically changes local security policies, and alerts you to changes you need to make to domain security policies. You can also change your security policies before installation. See How to assign user rights to the Windows Security Policies for Symantec Endpoint Protection Manager services.

Note: If you install Symantec Endpoint Protection Manager 14.2 in an IPv6 network, you must also have the IPv4 stack available for Java, even if IPv4 is disabled. If the IPv4 stack is uninstalled, Java does not work, and the Symantec Endpoint Protection Manager installation fails.

To install Symantec Endpoint Protection Manager

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

   If you have a product disc, insert it into the optical drive. The installation should start automatically. If it does not start, open the disc, and then double-click **Setup.exe**.

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 management server 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 Symantec Endpoint Protection Manager after installation" on page 44.

See "Installing Symantec Endpoint Protection Manager with a custom configuration" on page 45.

See "Choosing a method to install the client using the Client Deployment Wizard" on page 119.

See "Preparing for client installation" on page 107.

See "Getting up and running on Symantec Endpoint Protection for the first time" on page 36.

Configuring Symantec Endpoint Protection Manager after installation

The Management Server Configuration Wizard automatically starts after the Symantec Endpoint Protection Manager installation. You configure the management server according to your requirements.

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 Symantec Endpoint Protection Manager after installation

1 See "Installing Symantec Endpoint Protection Manager" on page 43.

2 With the **Default Configuration** selected, click **Next**.

3 Enter company name, a password for the default administrator admin, and an email address.

Alternately, you can add details to use a specified mail server.

4 Click **Send Test Email**.

Symantec Endpoint Protection Manager sends password recovery information and other important notifications to this email account, so you should not proceed with configuration if you do not receive the email.

5 Once you verify that you receive the test email, click **Next**.

6 Indicate whether you want to run LiveUpdate as part of the installation. If you run LiveUpdate as part of a new installation, content is more readily available for the clients you deploy. Click **Next**

   You can also add the optional **Partner Information**, if a partner manages your Symantec licenses.

7 Indicate whether you want Symantec to receive pseudonymous data, and then click **Next** to begin the database creation.

8 When the database creation completes, click **Finish** to complete the Symantec Endpoint Protection Manager configuration.

   The Symantec Endpoint Protection Manager console logon screen appears if you leave the option checked to launch Symantec Endpoint Protection Manager. Once you log on, you can begin client deployment.

   See "Logging on to the Symantec Endpoint Protection Manager console" on page 48.

You can find a configuration summary in the following location on the server where Symantec Endpoint Protection Manager is installed:

ProgramFiles\Symantec\Symantec Endpoint Protection Manager\tomcat\etc\SEPMConfigurationSummaryInfo.txt

See "About choosing a database type" on page 85.

Installing Symantec Endpoint Protection Manager with a custom configuration

When you want to install Symantec Endpoint Protection Manager with a Microsoft SQL Server database and have more than 500 clients, you should choose **Custom configuration** in the **Management Server Configuration Wizard**. When you select this option, additional settings become available for configuration.

Note: To provide connectivity to the database, you must install SQL Server client tools on the server that runs Symantec Endpoint Protection Manager.

See "About SQL Server configuration settings" on page 87.

To install Symantec Endpoint Protection Manager with a custom configuration

1. See "Installing Symantec Endpoint Protection Manager" on page 43.
2. In the **Management Server Configuration Wizard**, click **Custom configuration**, and then click **Next**.

   If you have fewer than 500 clients, Symantec recommends that you click **Default configuration**.

   See "Configuring Symantec Endpoint Protection Manager after installation" on page 44.
3. Click **Install my first site**, and then click **Next**.

   The following options are for advanced installations and do not apply to first-time installations of Symantec Endpoint Protection Manager:

   - For **Install an additional management server to an existing site**, see Setting up failover and load balancing.
   - For **Install an additional site**, see:
     Setting up sites and replication
     How replication works
4. On this screen, you can customize the following settings, and then click **Next**:
   - Site name
   - Server name
   - Port numbers
     You should contact your network administrator before you make changes to the default Symantec Endpoint Protection Manager port configurations.
   - The location of the Symantec Endpoint Protection Manager server data folder
     If there is not enough available free space on the drive on which Symantec Endpoint Protection Manager is installed, relocate the server data folder to an alternate drive.
5. On the database selection screen, click **Microsoft SQL Server database** and then click **Next**.
   - You can select the embedded database with a custom configuration. However, this step assumes that you select the SQL Server database.
   - Check with your SQL database administrator to confirm whether or not the automatic database maintenance tasks should be enabled.
   - Symantec recommends that you host SQL Server and Symantec Endpoint Protection Manager on separate physical servers.
   - For information on supported versions of Microsoft SQL Server, see the system requirements for Symantec Endpoint Protection.

6 Click **Create a new database**, and then click **Next**.

Note: Using an existing database is considered an advanced installation option, and typically does not apply to new installations.

7 On the **Step One: Database Server Authentication** screen, fill in the details for the SQL Server to which Symantec Endpoint Protection Manager connects, and then click **Connect to database**.

If the database connection is successful, the **Step Two: New Database Creation** section becomes available.

8 Under **Step Two: New Database Creation**, fill in the details to create a new database, and then click **Next**.

For questions regarding either **Database Server Authentication** or **Database Creation**, contact your SQL Server database administrator.

9 Enter company name, a password for the default administrator admin, and an email address.

Alternately, you can add details to use a specified mail server.

10 Click **Send Test Email**. Once you verify that you receive the test email, click **Next**.

Symantec Endpoint Protection Manager sends password recovery information and other important notifications to this email account, so you should not proceed with configuration if you do not receive the email.

11 Create an encryption password, or choose to use a random password, and then click **Next**.

This password is used to protect the communication between clients and Symantec Endpoint Protection Manager, and is stored in the Symantec Endpoint Protection Manager recovery file.

12 Indicate whether you want to run LiveUpdate as part of the installation. If you run LiveUpdate as part of a new installation, content is more readily available for the clients you deploy. Click **Next**

You can also add the optional **Partner Information**, if a partner manages your Symantec licenses.

13 Indicate whether you want Symantec to receive pseudonymous data, and then click **Next** to begin the database creation.

14 After the database is created and initialized (which may take several minutes), click **Finish**.

The Symantec Endpoint Protection Manager console logon screen appears if you leave the option checked to launch Symantec Endpoint Protection Manager. Once you log on, you can begin client deployment.

See "Logging on to the Symantec Endpoint Protection Manager console" on page 48.

You can find a configuration summary in the following location on the server where Symantec Endpoint Protection Manager is installed:

ProgramFiles\Symantec\Symantec Endpoint Protection Manager\tomcat\etc\SEPMConfigurationSummaryInfo.txt

See "About choosing a database type" on page 85.

Logging on to the Symantec Endpoint Protection Manager console

You 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 you installed the management server.
  Logging on to the console locally
  You can also access the reporting functions from a standalone web browser that is connected to your management server.
  See "Logging on to reporting from a standalone web browser" on page 635.
- 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.
  Logging on to the console remotely

For security, the console logs you out after a maximum of one hour. You can decrease this period of time. In version 12.1.4 and earlier, you can disable the timeout period.

See "Changing the timeout period for staying logged on to the Symantec Endpoint Protection Manager console" on page 304.

Logging on to the console locally

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.

   Optionally check **Remember my user name**, **Remember my password** or both, if available.

   See "Displaying the Forgot your password? link so that administrators can reset lost passwords" on page 299.

   - To log on using a PIV card or CAC, click **Options**, and then check **Log on to a smart card** (as of 14.2). In the **Login / PIN** message, type your pin number.
     See "Configuring Symantec Endpoint Protection Manager to authenticate administrators who log on with smart cards" on page 289.
   - To log on using two-factor authentication, type the password immediately followed by the token. If you omit the token, the logon attempt fails. If you use the Symantec VIP smartphone app, type the password, and then approve the request on the app after you click **Log On**. If you do not approve the request within two minutes, the logon attempt fails.
     See "Configuring two-factor authentication with Symantec VIP" on page 288.

   If the console has more than one domain, click **Options** and type the domain name. See "Adding a domain" on page 308.
3. Click **Log On**.

Logging on to the console remotely

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.

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.

Note: For Windows Server 2016, use the host name of the computer on which the management server is installed.

To log on to the console remotely

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

   http://*SEPMServer*:9090

   Where *SEPMServer* is the host name or IP address of the management server. For a list of supported web browsers, see Release notes, new fixes, and system requirements for all versions of Endpoint Protection.

   IP address includes IPv4 and IPv6. You must enclose the IPv6 address with square brackets. For example: **http://[*SEPMServer*]:9090**

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 other option is not a remote management solution. You can click **Symantec Endpoint Protection Manager Certificate** to prompt 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 webpage 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.

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

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.

5 If you use the Java-based console, you may have the option to save the user name and password. 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 console requires.

See "Granting or blocking access to remote Symantec Endpoint Protection Manager consoles" on page 302.

See "Displaying a message for administrators to see before logging on to the Symantec Endpoint Protection Manager console" on page 301.

See "About accepting the self-signed server certificate for Symantec Endpoint Protection Manager" on page 300.

Activating or importing your Symantec Endpoint Protection 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 an additional paid license in response to an over-deployment status.

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

- MySymantec
- Symantec partner or preferred reseller
- Symantec sales team
- Symantec Business Store

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

- The Getting Started screen that appears after you install the product.
  You can also access the Getting Started screen through **Help > Getting Started Page**.
- The **Admin** page of the Symantec Endpoint Protection Manager console.

If you activate or import your license from the Getting Started screen, you can skip to step 3.

To activate or import your Symantec Endpoint Protection product license

1. In Symantec Endpoint Protection Manager, click **Admin > Licenses**.
2. Under **Tasks**, click **Activate license**.
3. Click **Activate a new license**, and then click **Next**. If you do not see this panel, continue to the next step.
4. 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, you receive a Symantec license file (.slf file) 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 webpage:

   Enterprise Options
5. 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**.

Note: To activate a license with a serial number, you must have an active internet connection and be able to reach the Symantec Licensing Server. If the connection succeeds, the Symantec home page loads. If the connection fails, see the following:

How to test connectivity with Insight and Symantec Licensing servers

- 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 came with your Symantec notification email. Click **Open**, and then click **Next**.

6 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.

7 Click **Finish**.

See "About the trial license" on page 96.

See "About renewing your Symantec Endpoint Protection license" on page 99.

See "About purchasing Symantec Endpoint Protection licenses" on page 97.

See "Licensing Symantec Endpoint Protection" on page 94.

Installing Symantec Endpoint Protection clients with Save Package

If you have a small number of clients, use the Save Package method to deploy and install the installation package on the clients.

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

Save Package comprises the following tasks:

- You make your configuration selections and then create the client installation packages.
- You save the installation package to a folder on the computer that runs Symantec Endpoint Protection Manager.
  For Windows, the installation package can be for 32- or 64-bit operating systems. The installation package comprises 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.

Note: The Mac and Linux client install packages automatically export a `.zip` archive file format. To correctly preserve the file permissions, you should expand the archive file with a native archive program, such as 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 the files for these operating systems.

To install Symantec Endpoint Protection clients with Save Package

1. In the console, launch the **Client Deployment Wizard**.

   Click **Help > Getting Started Page** and then under **Required tasks**, click **Install the client software on your computers**.

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

   - Click **New Package Deployment**, and then click **Next**. Save Package only installs a new installation package.
   - Click **Communication Update Package Deployment** if you want to update Windows or Mac client communication settings on the computers that already have the Symantec Endpoint Protection client installed. Follow the on-screen instructions, and then go to step 4.

3. Make selections from the available options, which vary depending on the installation package type, and then click **Next**.

   Note: To uninstall existing security software on the Windows client, you must configure custom Client Install Settings before launching the Client Deployment Wizard.

   See "Configuring client packages to uninstall existing security software" on page 124.

   See "About the Windows client installation settings" on page 123.

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

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

   For Communication Update Package Deployment, or for Mac and Linux packages, go to step 6.

   For new Windows packages, check **Single .exe file (default)** or **Separate files (required for .MSI)**.

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

6. Click **Next**.

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

8 Provide the exported package to the computer users.

Provide the exported package to the users in the following ways: email, save the package to a secure shared network location, or use a third-party program.

9 Confirm that the user downloads and installs the client software, and confirm the installation status of the clients.

For new Symantec Endpoint Protection installations, the client computers may not appear within Symantec Endpoint Protection Manager until after they restart, either automatically or by action you or the user takes. Mac clients automatically prompt a restart when installation completes. Linux clients do not require a restart.

See "Restarting the client computers from Symantec Endpoint Protection Manager" on page 127.

See "Running a report on the deployment status of clients" on page 631.

See "Choosing which security features to install on the client" on page 121.

See "Choosing a method to install the client using the Client Deployment Wizard" on page 119.

See "Preparing for client installation" on page 107.

Installing the Symantec Endpoint Protection client for Mac

You can directly install a Symantec Endpoint Protection client on a Mac computer if you cannot use or do not want to use Remote Push. The steps are similar whether the client is unmanaged or managed.

The only way to install a managed client is with a package that Symantec Endpoint Protection Manager creates. You can convert an unmanaged client to a managed client at any time by importing client-server communication settings into the Mac client.

Note: To prepare the Symantec Endpoint Protection client for Mac for use with third-party remote deployment software, see Exporting and Deploying a Symantec Endpoint Protection client via Apple Remote Desktop or Casper.

If you downloaded the installation file or received a product disc

1 Perform one of the following tasks:

If you downloaded the installation file, extract the contents to a folder on a Mac computer, and then open the folder.

If you received a disc, insert it into a computer.

2 Open `SEP_MAC`.

3 Copy `Symantec Endpoint Protection.dmg` to the desktop of the Mac computer.

4 Double-click `Symantec Endpoint Protection.dmg` to mount the file as a virtual disk. You then install the Symantec Endpoint Protection client for Mac.

If you have a client installation package .zip

1 If you exported the installation package or downloaded the client installer package from MySymantec, copy the file to the desktop of the Mac computer.

The file may be named `Symantec Endpoint Protection.zip` or `Symantec_Endpoint_Protection_`*`version`*`_Mac_Client.zip`, where *version* is the product version.

2 Right-click **Open With > Archive Utility** to extract the file's contents.

3 Open the resulting folder. You then install the Symantec Endpoint Protection client for Mac.

Note: The resulting virtual disk image or folder contains the application installer and a folder called **Additional Resources**. Both items must be present in the same location for a successful installation. If you copy the installer to another location, you must also copy **Additional Resources**.

To install the Symantec Endpoint Protection client for Mac

1 Double-click **Symantec Endpoint Protection Installer**.

2 To acknowledge the required restart, click **Continue**.

3 To review the license agreement, click **View License Agreement**.

To begin the installation, click **Agree & Install**.

4 Enter the user name and password for the Mac administrative account when prompted, and then click **Install Helper**.

5 To authorize the Symantec Endpoint Protection kernel extension for macOS 10.13, in the installer pane, click **System Preferences**, and then in the **Security & Privacy** system preference pane, click **Allow**. You do not need to enter a password.

6 In the installer pane, click **Close & Restart** to complete the installation.

When you log back on to the Mac computer, LiveUpdate launches to update the definitions. LiveUpdate runs silently in the background and does not display its progress onscreen.

If you were prompted to authorize the kernel extension but did not do it in step 5, do so after the computer restarts. You must authorize the kernel extension for Symantec Endpoint Protection to fully function.

See "About authorizing kernel extensions for Symantec Endpoint Protection for macOS 10.13 or later" on page 57.

See "Exporting client installation packages" on page 136.

See "Restoring client-server communications with Communication Update Package Deployment" on page 173.

See "Installing Symantec Endpoint Protection clients with Save Package" on page 53.

See "Installing Symantec Endpoint Protection clients with Remote Push" on page 60.

About authorizing kernel extensions for Symantec Endpoint Protection for macOS 10.13 or later

Requiring the authorization of kernel extensions (kexts) is a new security feature as of macOS 10.13. Symantec Endpoint Protection 14.0.1 adds support for macOS 10.13. You must authorize the kernel extension for Symantec Endpoint Protection to fully function.

During installation of the client, click **Allow** when you are prompted under **System Preferences** in the **Security & Privacy** system preference pane. You do not need to enter a password.

The option to allow the Symantec Endpoint Protection kernel extensions in the System Preferences disappears after 30 minutes. You can get the option back in the following ways:

- Restart the Mac. You can then open the **Security & Privacy** system preference.
- Open the Symantec Endpoint Protection client user interface on the Mac and click **Fix** next to the message **Kernel extensions need authorization**. This action opens the **Security & Privacy** system preference.

If you have previously authorized the Symantec Endpoint Protection kernel extension on the Mac computer, you do not need to authorize it again. For example, you do not have to authorize the kernel extension again if you uninstall and then reinstall the client. You also do not have to explicitly authorize if you upgrade Symantec Endpoint Protection to 14.0.1 and then upgrade the operating system to macOS 10.13.

However, you need to reauthorize the kernel extension if you reinstall the operating system. You must also reauthorize the kernel extension if you upgrade from a Symantec Endpoint Protection version earlier than 14.2 to version 14.2 or later.

See "Managing kernel extension authorization when deploying the Symantec Endpoint Protection client for Mac" on page 58.

See "Installing the Symantec Endpoint Protection client for Mac" on page 55.

Managing kernel extension authorization when deploying the Symantec Endpoint Protection client for Mac

If you mass-deploy the Symantec Endpoint Protection client for Mac, you may need to take additional steps to ensure that the kernel extensions are authorized. This requirement applies as of macOS 10.13 (High Sierra). The operating system dictates that the authorization must be made at the local computer. You cannot authorize the kernel extension through remote access, nor can you save the kernel authorization through a preconfigured disk image.

To ensure that kernel extensions are properly authorized on Macs, do one of the following:

- Instruct the Mac users to approve the required extension. Any user can approve a kernel extension through the Security & Privacy preference pane, even if they do not have administrator privileges.
  See "About authorizing kernel extensions for Symantec Endpoint Protection for macOS 10.13 or later" on page 57.
- Enroll your Macs in a mobile device management (MDM) solution. Even if you do not actively manage Macs with this solution, kernel extension authorization reverts to the way it was enforced before macOS 10.13.
- As of macOS 10.13.2, authorize the kernel extensions through mobile device management (MDM) with the use of a team identifier. To authorize the kernel extensions for Symantec Endpoint Protection on macOS, use the team identifier `9PTGMPNXZ2`. Consult the documentation for your MDM suite for guidance on how to use this team identifier.
- If you use **NetBoot**, **NetInstall**, or **NetRestore**, use the following command while preparing disk images for deployment:

  ```
  spctl kext-consent add 9PTGMPNXZ2
  ```

  This command uses the Symantec team identifier to pre-approve Symantec kernel extensions on Mac.

  Team identifiers that are set through this command are stored in non-volatile random-access memory (NVRAM), which persists even when the Mac powers off. If you reset the NVRAM, the kernel extensions require reapproval. If the user also approved the kernel extension through the Security & Privacy pane, then reapproval is not needed.

For more information on kernel extension loading, see the following Apple documentation:

Prepare for changes to kernel extensions in macOS High Sierra

Installing the Symantec Endpoint Protection client for Linux

You install an unmanaged or managed Symantec Endpoint Protection client directly on a Linux computer. You cannot deploy the Linux client from Symantec Endpoint Protection Manager remotely. The installation steps are similar whether the client is unmanaged or managed.

The only way to install a managed client is with an installation package that you create in Symantec Endpoint Protection Manager. You can convert an unmanaged client to a managed client at any time by importing client-server communication settings into the Linux client.

If the Linux operating system kernel is incompatible with the pre-compiled Auto-Protect kernel module, the installer tries to compile a compatible Auto-Protect kernel module. The auto-compile process automatically launches if it is needed. However, the installer might be unable to compile a compatible Auto-Protect kernel module. In this case, Auto-Protect installs but is disabled. For more information, see:

Supported Linux kernels for Symantec Endpoint Protection

Note: You must have superuser privileges to install the Symantec Endpoint Protection client on the Linux computer. The procedure uses `sudo` to demonstrate this elevation of privilege.

To install the Symantec Endpoint Protection client for Linux

1. Copy the installation package that you created to the Linux computer. The package is a .zip file.
2. On the Linux computer, open a terminal application window.
3. Navigate to the installation directory with the following command:

   `cd /directory/`

   Where *directory* is the name of the directory into which you copied the .zip file.
4. Extract the contents of the .zip file into a directory named `tmp` with the following command:

   `unzip "InstallPackage" -d sepfiles`

   Where *`InstallPackage`* is the full name of the .zip file, and *`sepfiles`* represents a destination folder into which the extraction process places the installation files.

   If the destination folder does not exist, the extraction process creates it.
5. Navigate to *`sepfiles`* with the following command:

   `cd sepfiles`

6 To correctly set the execute file permissions on `install.sh`, use the following command:

```
chmod u+x install.sh
```

7 Use the built-in script to install Symantec Endpoint Protection with the following command:

```
sudo ./install.sh -i
```

Enter your password if prompted.

This script initiates the installation of the Symantec Endpoint Protection components. The default installation directory is as follows:

```
/opt/Symantec/symantec_antivirus
```

The default work directory for LiveUpdate is as follows:

```
/opt/Symantec/LiveUpdate/tmp
```

The installation completes when the command prompt returns. You do not have to restart the computer to complete the installation.

To verify the client installation, click or right-click the Symantec Endpoint Protection yellow shield and then click **Open Symantec Endpoint Protection**. The location of the yellow shield varies by Linux version. The client user interface displays information about program version, virus definitions, server connection status, and management.

See "Importing client-server communication settings into the Linux client" on page 175.

See "Preparing for client installation" on page 107.

Installing Symantec Endpoint Protection clients with Remote Push

Remote Push pushes the client software to the computers that you specify, either by IP address or by computer names. Once the package copies to the target computer, the package installs automatically. The computer user does not need to begin the installation or to have administrator privileges.

Remote Push comprises the following tasks:

- You select an existing client installation package, create a new installation package, or create a package to update communication settings.
- For new installation packages, you configure and create the installation package.
- You specify the computers on your network to receive a package from Symantec Endpoint Protection Manager.
  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.

Note: To push the client installation package to Mac clients in the **Browse Network** tab, you must install the Bonjour service on the Symantec Endpoint Protection Manager server. See the following article:

Installing the Bonjour Service for Symantec Endpoint Protection Manager 12.1.5 or later

The Bonjour service does not support IPv6 networking. Macs that only have IPv6 networking enabled cannot display in **Browse Network**.

- Symantec Endpoint Protection Manager pushes the client software to the specified computers.
  The installation automatically begins on the computers once the package successfully copies to the target computer.

Note: You cannot install the Linux client with Remote Push.

To install Symantec Endpoint Protection clients with Remote Push

1. In the console, launch the **Client Deployment Wizard**.
   Click **Help > Getting Started Page** and then under **Required tasks**, click **Install the client software on your 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 install.
     The Client Deployment Wizard uploads the package and directs you to the **Computer Selection** panel (step 5).
   - Under **Communication Update Package Deployment**, choose whether to update Windows or Mac client communication settings on the computers that already have the Symantec Endpoint Protection client installed. Follow the on-screen instructions, and then go to step 4.
     Use this option to convert an unmanaged client to a managed client.

   See “Restoring client-server communications with Communication Update Package Deployment” on page 173.

3 For a new package, in the **Select Group and Install Feature Sets** panel, make selections from the available options, which vary depending on the installation package type. Click **Next**.

Note: To uninstall existing security software on the Windows 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.

See "Configuring client packages to uninstall existing security software" on page 124.

See "About the Windows client installation settings" on page 123.

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 installed clients on the **Clients** page.

For new Symantec Endpoint Protection installations, the client computers may not appear within Symantec Endpoint Protection Manager until after they restart, either automatically or by action you or the user takes.

See "Restarting the client computers from Symantec Endpoint Protection Manager" on page 127.

See "Running a report on the deployment status of clients" on page 631.

Note: After you remotely install the client installation package to Mac clients, you must verify on the client computer that the kernel extension is authorized. Kernel extension authorization is required for Symantec Endpoint Protection to fully function, and Remote Push does not prompt you to authorize if authorization is needed. On the Mac, check the **Security & Privacy** system preference, and click **Allow**.

See "Preparing for client installation" on page 107.

See "Preparing Windows and Mac computers for remote deployment" on page 108.

See "Choosing which security features to install on the client" on page 121.

See "Choosing a method to install the client using the Client Deployment Wizard" on page 119.

Installing Symantec Endpoint Protection clients with Web Link and Email

The Web Link and Email option creates the installation package and the URL for the installation package. The users receive the URL in an email to download the package and install the Symantec Endpoint Protection client. Users must have administrator privileges to install the package.

Web Link and Email comprises the following tasks:

- You select, configure, and then create the client installation package.
  You choose from the options that appear for the configuration of Windows, Mac, and Linux client installation packages. All client installation packages are stored on the computer that runs Symantec Endpoint Protection Manager.
- Email from Symantec Endpoint Protection Manager notifies the computer users that they can download the client installation package.
  You provide a list of users to receive an email message, which contains instructions to download and install the client installation package. Users follow the instructions to install the client software.

Note: The Mac and the Linux client install packages automatically export a `.zip` archive file format. To correctly preserve the file permissions, you should expand the archive file with a native archive program, such as 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 the files for these operating systems.

Before you use Web Link and Email, make sure that you correctly configure the connection from the management server to the mail server.

See "Establishing communication between the management server and email servers" on page 668.

To install Symantec Endpoint Protection clients with Web Link and Email

1. In the console, launch the **Client Deployment Wizard**.

   Click **Help > Getting Started Page** and then under **Required tasks**, click **Install the client software on your computers**.

2. In the **Client Deployment Wizard**, click **New Package Deployment**, and then click **Next**. Web Link and Email only sends a new installation package.

3. Make selections from the available options, which vary depending on the installation package type, and then click **Next**.

   Note: To uninstall existing security software on the Windows client, you must configure custom Client Install Settings before launching the Client Deployment Wizard.

   See "Configuring client packages to uninstall existing security software" on page 124.

   See "About the Windows client installation settings" on page 123.

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 and secure online location, like an intranet page.

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

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

   Client computers may not appear within Symantec Endpoint Protection Manager until after they restart, either automatically or by action you or the user takes. Mac clients automatically prompt a restart when installation completes. Linux clients do not require a restart.

   See "Restarting the client computers from Symantec Endpoint Protection Manager" on page 127.

   See "Running a report on the deployment status of clients" on page 631.

See "Choosing which security features to install on the client" on page 121.

See "Choosing a method to install the client using the Client Deployment Wizard" on page 119.

See "Preparing for client installation" on page 107.

What do I do after I install the management server?

Table 2-1 displays the tasks to perform after you install and configure the product to assess whether the client computers have the correct level of protection. Continue to perform these tasks regularly, on a weekly or monthly basis.

Table 2-1 Tasks to perform 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 432. ■ Enable Risk Tracer in Auto-Protect. For more information, see the article: What is Risk Tracer? Risk Tracer has the following prerequisites: ■ Network Threat Protection is enabled. See "Running commands on client computers from the console" on page 253. ■ Windows File and Printer Sharing is enabled. See "Customizing Auto-Protect for Windows clients" on page 468.
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 362. See "Managing locations for remote clients" on page 263.

Table 2-1 Tasks to perform 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 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 SQL Server database files. These exceptions improve performance and avoid corruption or files being locked when SQL Server must use them. For more information, see the knowledge base article: How to exclude MS SQL files and folders using Centralized Exceptions. In addition, you should exclude false positives from scans. You can also exclude files by extension for Auto-Protect scans on Windows computers. See "Creating exceptions for Virus and Spyware scans" on page 548. See "Customizing Auto-Protect for Windows clients" on page 468. See "Customizing Auto-Protect for Mac clients" on page 470.
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 Symantec Endpoint Protection Manager reports" on page 637. See "Running and customizing quick reports" on page 649. See "How to run scheduled reports" on page 652.
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 625.

Table 2-1 Tasks to perform after you install *(continued)*

Action	Description
Assess your content storage and client communication bandwidth requirements	As of 12.1.5, Symantec Endpoint Protection Manager no longer stores multiple full content versions. Instead, only the latest full version plus incremental deltas are stored. This approach means that clients almost always download deltas, not full packages. Only in the rare case where a client is extremely out of date (more than three months), is a full download of the latest content required. If your environment must control network bandwidth precisely, you can also throttle client communication. For more information, see the article: Symantec Endpoint Protection Bandwidth Control for Client Communication See "How to update content and definitions on the clients" on page 178. 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 671. See "Managing notifications" on page 661.

See "Getting up and running on Symantec Endpoint Protection for the first time" on page 36.

See: Symantec Endpoint Protection Recommended Best Practices for Securing an Enterprise Environment

Chapter 3

System requirements

This chapter includes the following topics:

- System requirements for Symantec Endpoint Protection
- Symantec Endpoint Protection product license requirements
- Supported virtual installations and virtualization products

System requirements for Symantec Endpoint Protection

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

Note: For the most current system requirements, see:

System requirements for Symantec Endpoint Protection 14.2 RU1

When information conflicts, the webpage should be considered the most accurate.

- See “Symantec Endpoint Protection Manager system requirements” on page 69.
- See “Symantec Endpoint Protection client for Windows system requirements” on page 72.
- See “Symantec Endpoint Protection client for Windows Embedded system requirements” on page 75.
- See “Symantec Endpoint Protection client for Mac system requirements” on page 77.
- See “Symantec Endpoint Protection client for Linux system requirements” on page 77.

See “Getting up and running on Symantec Endpoint Protection for the first time” on page 36.

See “Supported virtual installations and virtualization products” on page 81.

See “Internationalization requirements” on page 78.

Symantec Endpoint Protection Manager system requirements

The following tables describe the software and hardware requirements for Symantec Endpoint Protection Manager.

Table 3-1 Symantec Endpoint Protection Manager software system requirements

Component	Requirements
Operating system	■ Windows Server 2008 R2 ■ Windows Server 2012 ■ Windows Server 2012 R2 ■ Windows Server 2016 ■ Windows Server 2019 **Note:** Desktop operating systems are not supported. Windows Server Core edition is not supported. Windows Server Core does not include Internet Explorer, which Symantec Endpoint Protection Manager requires to work.
Web browser	The following browsers are supported for web console access to Symantec Endpoint Protection Manager and for viewing the Symantec Endpoint Protection Manager Help: ■ Microsoft Edge Note: The 32-bit version Windows 10 does not support web console access on the Edge browser. ■ Microsoft Internet Explorer 11 ■ Mozilla Firefox 5.x through 66.x ■ Google Chrome 73.x

Table 3-1 Symantec Endpoint Protection Manager software system requirements *(continued)*

Component	Requirements
Database	The Symantec Endpoint Protection Manager includes an embedded database. You may instead choose to use a database from one of the following versions of Microsoft SQL Server: ■ SQL Server 2008, SP4 ■ SQL Server 2008 R2, SP3 ■ SQL Server 2012, RTM - SP4 ■ SQL Server 2014, RTM - SP2 ■ SQL Server 2016, RTM, SP1 ■ SQL Server 2017, RTM **Note:** The SQL Server Express Edition database is not supported. SQL Server databases that are hosted on Amazon RDS are supported. **Note:** If Symantec Endpoint Protection uses a SQL Server database and your environment only uses TLS 1.2, ensure that SQL Server supports TLS 1.2. You may need to patch SQL Server. This recommendation applies to SQL Server 2008, 2012, and 2014. For more information: TLS 1.2 support for Microsoft SQL Server
Other environmental requirements	In purely IPv6 networks, the IPv4 stack must still be installed and disabled. If the IPv4 stack is uninstalled, Symantec Endpoint Protection Manager does not work.

Table 3-2 Symantec Endpoint Protection Manager hardware system requirements

Component	Requirements
Processor	Intel Pentium Dual-Core or equivalent minimum, 8-core or greater recommended **Note:** Intel Itanium IA-64 processors are not supported.
Physical RAM	2 GB RAM available minimum; 8 GB or more available recommended **Note:** Your Symantec Endpoint Protection Manager server may require additional RAM depending on the RAM requirements of other applications that are already installed. For example, if Microsoft SQL Server is installed on the Symantec Endpoint Protection Manager server, the server should have a minimum of 8 GB available.
Display	1024 x 768 or larger

Table 3-2 Symantec Endpoint Protection Manager hardware system requirements *(continued)*

Component	Requirements
Hard drive when installing to the system drive	With an embedded database or a local SQL Server database: ■ 40 GB available minimum (200 GB recommended) for the management server and database With a remote SQL Server database: ■ 40 GB available minimum (100 GB recommended) for the management server ■ Additional available disk space on the remote server for the database
Hard drive when installing to an alternate drive	With an embedded database or a local SQL Server database: ■ The system drive requires 15 GB available minimum (100 GB recommended) ■ The installation drive requires 25 GB available minimum (100 GB recommended) With a remote SQL Server database: ■ The system drive requires 15 GB available minimum (100 GB recommended) ■ The installation drive requires 25 GB available minimum (100 GB recommended) ■ Additional available disk space on the remote server for the database

Note: If you use a SQL Server database, you may need to make more disk space available. The amount and location of additional space depends on which drive SQL Server uses, database maintenance requirements, and other database settings.

See "Supported virtual installations and virtualization products" on page 81.

Symantec Endpoint Protection client for Windows system requirements

Table 3-3 Symantec Endpoint Protection client for Windows software system requirements

Component	Requirements
Operating system (desktop)	■ Windows 7 (32-bit, 64-bit; RTM and SP1) ■ Windows Embedded 7 Standard, POSReady, and Enterprise (32-bit and 64-bit) ■ Windows 8 (32-bit, 64-bit) ■ Windows Embedded 8 Standard (32-bit and 64-bit) ■ Windows 8.1 (32-bit, 64-bit), including Windows To Go ■ Windows 8.1 update for April 2014 (32-bit, 64-bit) ■ Windows 8.1 update for August 2014 (32-bit, 64-bit) ■ Windows Embedded 8.1 Pro, Industry Pro, and Industry Enterprise (32-bit and 64-bit) ■ Windows 10 (version 1507) (32-bit, 64-bit), including Windows 10 Enterprise 2015 LTSB ■ Windows 10 November Update (version 1511) (32-bit, 64-bit) ■ Windows 10 Anniversary Update (version 1607) (32-bit, 64-bit), including Windows 10 Enterprise 2016 LTSB ■ Windows 10 Creators Update (version 1703) (32-bit, 64-bit) ■ Windows 10 Fall Creators Update (version 1709) (32-bit, 64-bit) ■ Windows 10 April 2018 Update (version 1803) (32-bit, 64-bit) ■ Windows 10 October 2018 Update (version 1809) (32-bit, 64-bit) ■ Windows 10 May 2019 Update (version 1903) (32-bit, 64-bit) See “Symantec Endpoint Protection client for Windows Embedded system requirements” on page 75.
Operating system (server)	■ Windows Server 2008 (32-bit, 64-bit; RTM, R2, SP1, and SP2) Includes Windows Small Business Server 2008 (64-bit) and Windows Essential Business Server 2008 (64-bit) ■ Windows Small Business Server 2011 (64-bit) ■ Windows Server 2012 ■ Windows Server 2012 R2 ■ Windows Server 2012 R2 update for April 2014 ■ Windows Server 2012 R2 update for August 2014 ■ Windows Server 2016 ■ Windows Server 2019

Table 3-4 Symantec Endpoint Protection client for Windows hardware system requirements

Component	Requirements
Processor (for physical computers)	■ 32-bit processor: 2 GHz Intel Pentium 4 or equivalent minimum (Intel Pentium 4 or equivalent recommended) ■ 64-bit processor: 2 GHz Pentium 4 with x86-64 support or equivalent minimum **Note:** Itanium processors are not supported.
Processor (for virtual computers)	One virtual socket and one core per socket at 1 GHz minimum (one virtual socket and two cores per socket at 2 GHz recommended) **Note:** The hypervisor resource reservation must be enabled.
Physical RAM	1 GB (2 GB recommended) or higher if required by the operating system
Display	800 x 600 or larger
Hard drive	Disk space requirements depend on the type of client you install, which drive you install to, and where the program data file resides. The program data folder is usually on the system drive in the default location C:\ProgramData. Available disk space is always required on the system drive, regardless of which installation drive you choose. Hard drive system requirements: ■ Table 3-5 describes the hard drive system requirements when Symantec Endpoint Protection is installed to the system drive. ■ Table 3-6 describes the hard drive system requirements when Symantec Endpoint Protection is installed to an alternate drive. **Note:** Space requirements are based on NTFS file systems. Additional space is also required for content updates and logs.

Table 3-5 Symantec Endpoint Protection client for Windows available hard drive system requirements when installed to the system drive

Client type	Requirements
Standard	With the program data folder located on the system drive: ■ 395 MB* With the program data folder located on an alternate drive: ■ System drive: 180 MB ■ Alternate installation drive: 350 MB

Table 3-5 Symantec Endpoint Protection client for Windows available hard drive system requirements when installed to the system drive *(continued)*

Client type	Requirements
Embedded / VDI	With the program data folder located on the system drive: ■ 245 MB* With the program data folder located on an alternate drive: ■ System drive: 180 MB ■ Alternate installation drive: 200 MB
Dark network	With the program data folder located on the system drive: ■ 545 MB* With the program data folder located on an alternate drive: ■ System drive: 180 MB ■ Alternate installation drive: 500 MB

* An additional 135 MB is required during installation.

Table 3-6 Symantec Endpoint Protection client for Windows available hard drive system requirements when installed to an alternate drive

Client type	Requirements
Standard	With the program data folder located on the system drive: ■ System drive: 380 MB ■ Alternate installation drive: 15 MB* With the program data folder located on an alternate drive:** ■ System drive: 30 MB ■ Program data drive: 350 MB ■ Alternate installation drive: 150 MB
Embedded / VDI	With the program data folder located on the system drive: ■ System drive: 230 MB ■ Alternate installation drive: 15 MB* With the program data folder located on an alternate drive:** ■ System drive: 30 MB ■ Program data drive: 200 MB ■ Alternate installation drive: 150 MB

Table 3-6 Symantec Endpoint Protection client for Windows available hard drive system requirements when installed to an alternate drive *(continued)*

Client type	Requirements
Dark network	With the program data folder located on the system drive: ■ System drive: 530 MB ■ Alternate installation drive: 15 MB* With the program data folder located on an alternate drive:** ■ System drive: 30 MB ■ Program data drive: 500 MB ■ Alternate installation drive: 150 MB

* An additional 135 MB is required during installation.

** If the program data folder is the same as the alternate installation drive, add 15 MB to the program data drive for your total. However, the installer still needs the full 150 MB to be available on the alternate installation drive during installation.

See "Supported virtual installations and virtualization products" on page 81.

System requirements for Symantec Endpoint Protection Hardening

Symantec Endpoint Protection client for Windows Embedded system requirements

Table 3-7 Symantec Endpoint Protection client for Windows Embedded system requirements

Component	Requirements
Processor	1 GHz Intel Pentium
Physical RAM	256 MB **Note:** This figure is for an installation of the Symantec Endpoint Protection embedded client. If you also implement additional features from an integrated solution such as Symantec Endpoint Detection and Response, additional physical RAM is needed.

Table 3-7 Symantec Endpoint Protection client for Windows Embedded system requirements *(continued)*

Component	Requirements
Hard drive	The Symantec Endpoint Protection Embedded / VDI client requires the following available hard disk space: ■ Installed to the system drive: 245 MB ■ Installed to an alternate drive: 230 MB on system drive, and 15 MB on the alternate drive An additional 135 MB is needed during installation. These figures assume that the program data folder is on the system drive. For more detailed information, or for the requirements of the other client types, see the Symantec Endpoint Protection client for Windows system requirements. See "Symantec Endpoint Protection client for Windows system requirements" on page 72.
Embedded operating system	■ Windows Embedded Standard 7 (32-bit and 64-bit) ■ Windows Embedded POSReady 7 (32-bit and 64-bit) ■ Windows Embedded Enterprise 7 (32-bit and 64-bit) ■ Windows Embedded 8 Standard (32-bit and 64-bit) ■ Windows Embedded 8.1 Industry Pro (32-bit and 64-bit) ■ Windows Embedded 8.1 Industry Enterprise (32-bit and 64-bit) ■ Windows Embedded 8.1 Pro (32-bit and 64-bit)
Required minimum components	■ Filter Manager (FltMgr.sys) ■ Performance Data Helper (pdh.dll) ■ Windows Installer Service
Templates	■ Application Compatibility (Default) ■ Digital Signage ■ Industrial Automation ■ IE, Media Player, RDP ■ Set Top Box ■ Thin Client The Minimum Configuration template is not supported. The Enhanced Write Filter (EWF) and the Unified Write Filter (UWF) are not supported. The recommended write filter is the File Based Write Filter (FBWF) installed along with the Registry Filter.

See Symantec Endpoint Protection support for Windows Embedded.

See "Supported virtual installations and virtualization products" on page 81.

Symantec Endpoint Protection client for Mac system requirements

Table 3-8 Symantec Endpoint Protection client for Mac system requirements

Component	Requirements
Processor	64-Bit Intel Core 2 Duo or later
Physical RAM	2 GB of RAM
Hard drive	500 MB of available hard disk space for the installation
Display	800 x 600
Operating system	Mac OS X 10.10, 10.11; macOS 10.12, 10.13, 10.14

Symantec Endpoint Protection client for Linux system requirements

Table 3-9 Symantec Endpoint Protection client for Linux system requirements

Component	Requirements
Hardware	■ Intel Pentium 4 (2 GHz) or later processor ■ 1 GB of RAM ■ 7 GB of available hard disk space
Operating systems	■ Amazon Linux ■ CentOS 6U3 - 6U9, 7 - 7U5; 32-bit and 64-bit ■ Debian 6.0.5 Squeeze, Debian 8 Jessie; 32-bit and 64-bit ■ Fedora 16, 17; 32-bit and 64-bit ■ Oracle Linux (OEL) 6U2, 6U4, 6U5, 6U8; 7, 7U1, 7U2, 7U3 ■ Red Hat Enterprise Linux Server (RHEL) 6U2 - 6U9, 7 - 7U5 ■ SUSE Linux Enterprise Server (SLES) 11 SP1 - 11 SP4, 32-bit and 64-bit; 12, 12 SP1 - 12 SP3, 64-bit ■ SUSE Linux Enterprise Desktop (SLED) 11 SP1 - 11 SP4, 32-bit and 64-bit; 12 SP3, 64-bit ■ Ubuntu 12.04, 14.04, 16.04, 18.04; 32-bit and 64-bit For a list of supported operating system kernels, see Supported Linux kernels for Symantec Endpoint Protection.
Graphical desktop environments	You can use the following graphical desktop environments to view the Symantec Endpoint Protection for Linux client: ■ KDE ■ Gnome ■ Unity

Table 3-9 Symantec Endpoint Protection client for Linux system requirements *(continued)*

Component	Requirements
Other environmental requirements	■ Glibc Any operating system that runs glibc earlier than 2.6 is not supported. ■ i686-based dependent packages on 64-bit computers Many of the executable files in the Linux client are 32-bit programs. For 64-bit computers, you must install the i686-based dependent packages before you install the Linux client. If you have not already installed the i686-based dependent packages, you can install them by command line. This installation requires superuser privileges, which the following commands demonstrate with `sudo`: ■ For Red Hat-based distributions: `sudo yum install glibc.i686 libgcc.i686 libX11.i686` ■ For Debian-based distributions: `sudo apt-get install ia32-libs` ■ For Ubuntu-based distributions: `sudo apt-get install libx11-6:i386 libgcc1:i386 libc6:i386` ■ net-tools or iproute2 Symantec Endpoint Protection uses one of these two tools, depending on what is already installed on the computer. ■ Developer tools Auto-compile and the manual compile process for the Auto-Protect kernel module require that you install certain developer tools. These developer tools include gcc and the kernel source and header files. For details on what to install and how to install them for specific Linux versions, see: Manually compile Auto-Protect kernel modules for Endpoint Protection for Linux

See "Supported virtual installations and virtualization products" on page 81.

Internationalization requirements

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

Table 3-10 Internationalization requirements

Component	Requirements
Computer names, server names, and workgroup 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, however. ■ 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 you provide feedback in the **User Information** client computer dialog box after you install the exported package. See "Collecting user information" on page 259.
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 product license" on page 51.

For the most current system requirements, see: Release notes, new fixes, and system requirements for all versions of Endpoint Protection

Symantec Endpoint Protection product license requirements

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

Table 3-11 Product license requirements

Product	Requirement
Paid license installation of Symantec Endpoint Protection 14	A 60-day trial license is included with Symantec Endpoint Protection. You must purchase a license that covers each deployed client when the trial license expires. One license covers all clients regardless of platform and version. See "How many Symantec Endpoint Protection licenses do I need?" on page 101.
Paid license installation of Symantec Endpoint Protection 12.1	Symantec Endpoint Protection accepts the license file from your previous Symantec virus protection software. You must purchase a new license when the previous 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 product license" on page 51.

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 product license" on page 51.

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.

Trial license	A trial license refers to a fully functioning installation of Symantec Endpoint Protection operating within the free evaluation period. If you want to continue using Symantec Endpoint Protection beyond the evaluation 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. The evaluation period is 60 days from the initial installation of Symantec Endpoint Protection Manager. See "About purchasing Symantec Endpoint Protection licenses" on page 97.
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 managing your product licenses after installation.

See "Getting up and running on Symantec Endpoint Protection for the first time" on page 36.

See "Licensing Symantec Endpoint Protection" on page 94.

See "About purchasing Symantec Endpoint Protection licenses" on page 97.

See "Activating or importing your Symantec Endpoint Protection product license" on page 51.

Supported virtual installations and virtualization products

You can install Symantec Endpoint Protection on the supported operating systems that run in virtual environments. Install Symantec Endpoint Protection on the guest operating system, and not the host.

The following virtualization products support the Symantec Endpoint Protection Manager, console, and embedded database components, and Symantec Endpoint Protection client software for Windows and Linux:

- Microsoft Azure
- Amazon WorkSpaces
- VMware WS 5.0 (workstation) or later
- VMware GSX 3.2 (enterprise) or later
- VMware ESX 2.5 (workstation) or later
- VMware ESXi 4.1 - 5.5
- VMware ESXi 6.0
- VMware ESXi 6.0 Update 1

- VMware ESXi 6.0 Update 2
- VMware ESXi 6.0 Update 3
- VMware ESXi 6.5
- VMware ESXi 6.5U1
- VMware ESXi 6.5U2
- VMware ESXi 6.7
- Microsoft Virtual Server 2005
- Windows Server 2008 Hyper-V
- Windows Server 2012 Hyper-V
- Windows Server 2012 R2 Hyper-V
- Windows Server 2016 Hyper-V
- Windows Server 2019 Hyper-V Core Edition
- Citrix XenServer 5.6 or later
- Virtual Box, supplied by Oracle

See "Using Symantec Endpoint Protection in virtual infrastructures" on page 675.

See "Randomizing scans to improve computer performance in virtualized environments on Windows clients" on page 477.

Section 1

Managing a custom installation

Chapter 4

Planning the installation

This chapter includes the following topics:

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.

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.

See "Getting up and running on Symantec Endpoint Protection for the first time" on page 36.

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 4-1 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 basic management server settings" on page 86.

Table 4-1 Databases that Symantec Endpoint Protection Manager uses *(continued)*

Database type	Description
SQL Server database	If you choose to use this option, you must install SQL Server and SQL Server Native Client before you install Symantec Endpoint Protection Manager. For optimal compatibility, you install the version of SQL Server Native Client equal to your version of SQL Server. You should consider purchasing and installing SQL Server for the following reasons: ■ You must support more than 5,000 clients. Each management server that uses SQL Server can support up to 18,000 clients (for 14.x) or 50,000 clients (for 12.1.x). If your organization has more 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 "Determining how many sites you need" on page 746. If you create a SQL Server database, you must first install an instance of SQL Server. You must then configure it for communication with the management server. See "About SQL Server configuration settings" on page 87.

About basic management server settings

The following values represent the default settings when you install the Symantec Endpoint Protection Manager.

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 43.

See "Communication ports for Symantec Endpoint Protection" on page 112.

Table 4-2 Basic server settings

Setting	Default	Description
Site Name	My Site (default) Site *local host name* (custom)	The name of the site as it appears in Symantec Endpoint Protection Manager. Site name is the highest-level container under which all features are configured and run within Symantec Endpoint Protection Manager.
Server name	*local host name*	The name of the computer that runs Symantec Endpoint Protection Manager.

Table 4-2 Basic server settings *(continued)*

Setting	Default	Description
Server data folder	*SEPM_Install*\data	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. The default value for *SEPM_Install* is C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager.
Encryption password	None	This password encrypts communication between Symantec Endpoint Protection Manager and clients. 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 "Disaster recovery best practices" on page 752.
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. You need the original admin password to reconfigure the management server at a later time. 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 SQL Server database, there are specific configuration requirements for SQL Server.

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: To maximize the security posture of remote SQL Server communications, place both servers in the same secure subnet.

Table 4-3 Required SQL Server configuration settings

Configuration setting	Installation requirement
Instance name	Do not use the default instance name. Create a name such as SEPM. By default, a database named Sem5 is created in the SQL Server instance when you install 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 91.
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 on the computer that runs Symantec Endpoint Protection Manager. SQL Server client components include `BCP.EXE`. The version number of the SQL Server client components should be the same as the version number of SQL Server that you use. Refer to your 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 4-4 displays the settings that you might need to know before you begin the installation process.

Table 4-4 SQL Server database settings

Setting	Default	Description
Server name	*local host name*	Name of the computer that runs Symantec Endpoint Protection Manager.
Server data folder	*SEPM_Install*\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. The default value for *SEPM_Install* is C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager.
Encryption password	None	The password that encrypts communication between Symantec Endpoint Protection Manager and clients. 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 "Disaster recovery best practices" on page 752.
Database server	*local host name*	Name of the computer where SQL Server is installed, 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*. The use of *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 Symantec Endpoint Protection Manager.
SQL Server Port	1433	The port that is used to send and receive traffic to the SQL Server. The use of port 0 is not supported. Port 0 specifies a random, negotiated port.
Database Name	sem5	Name of the database that is created.

Table 4-4 SQL Server database settings *(continued)*

Setting	Default	Description
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 native client folder	SQL Server 2008: *Install directory*\100\Tools\Binn SQL Server 2012: *Install directory*\110\Tools\Binn SQL Server 2014 / 2016: *Install directory*\Client SDK\ODBC\110\Tools\Binn	Location of the local SQL native client directory that contains bcp.exe. The installation paths that are shown represent the default paths for Microsoft SQL Server. *Install directory* represents the installation drive and directory for Microsoft SQL Server. To install the SQL Server native client, see the Microsoft TechNet page appropriate for your version of SQL Server: Installing SQL Server Native Client
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, which is typically sa.

Table 4-4 SQL Server database settings *(continued)*

Setting	Default	Description
Database data folder	Automatically detected after you click **Default**. SQL Server 2008: *Install directory*\MSSQL10.MSSQLSERVER\MSSQL\Data SQL Server 2008 R2: *Install directory*\MSSQL10_50.MSSQLSERVER\MSSQL\Data SQL Server 2012: *Install directory*\MSSQL11.MSSQLSERVER\MSSQL\Data SQL Server 2014: *Install directory*\MSSQL12.MSSQLSERVER\MSSQL\Data SQL Server 2016: *Install directory*\MSSQL13.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. The installation paths shown represent the default paths for Microsoft SQL Server. ■ 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 ■ If you install to a named instance on SQL Server 2014, the instance name is appended to MSSQL12. For example, \MSSQL12.*instance name*\MSSQL\Data ■ If you install to a named instance on SQL Server 2016, the instance name is appended to MSSQL13. For example, \MSSQL13.*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.

See "Installing Symantec Endpoint Protection Manager" on page 43.

About SQL Server database authentication modes

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

- Windows Authentication mode
- Mixed mode

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, 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 87.

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. To uninstall Symantec Endpoint Protection Manager, you use the Windows control panel for removing, repairing, or changing an application, typically **Programs and Features**.

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

In some cases, you may have to uninstall Symantec Endpoint Protection Manager using other methods, such as the CleanWipe utility. See:

Uninstall Symantec Endpoint Protection

See "Backing up the database and logs" on page 754.

Uninstalling Symantec Endpoint Protection with the CleanWipe utility

You can use several methods to uninstall the Symantec Endpoint Protection product components, such as through the Windows Control Panel. If these common methods fail, you can use the CleanWipe utility.

Warning: Symantec Technical Support does not recommend using CleanWipe the first time you have uninstallation trouble. You should only use CleanWipe as a last resort when the usual uninstallation methods are unsuccessful.

You should always use the latest version of CleanWipe to remove Symantec Endpoint Protection. CleanWipe can remove older installations of Symantec Endpoint Protection.

However, you should not use an older version of CleanWipe to remove a newer version of Symantec Endpoint Protection. This action can have unexpected results.

Note: CleanWipe removes security software installations of the Symantec enterprise product line, such as Symantec Endpoint Protection. To remove Symantec consumer products under the Norton brand, see:

Download and run the Norton Remove and Reinstall tool

As of 14, you can also incorporate CleanWipe functionality directly into the Symantec Endpoint Protection client package. You can enable this option with client installation settings. For more information, see About the Symantec Endpoint Protection client preinstall removal feature.

If you need help with CleanWipe, you can contact Technical Support directly.

To download CleanWipe from MySymantec, use the following guide:

Getting Started with MySymantec

To uninstall Symantec Endpoint Protection with the CleanWipe utility

1. Copy the folder that contains Cleanwipe.exe to the computer on which you want to run it.
2. Double-click Cleanwipe.exe, and then click **Next**.
3. Accept the license agreement, and then click **Next**.
4. Select the Symantec products you want to remove, and then click **Next** twice.
5. When the tool finishes running, you may be prompted to restart the computer.

   After the computer restarts, CleanWipe reopens and continues to run.
6. Click **Next**.
7. Click **Finish**.

   The Symantec products you selected are now uninstalled.

For information on recommended uninstallation methods, see:

Uninstall Symantec Endpoint Protection

About Symantec Endpoint Protection client installation failures and CleanWipe

Chapter 5

Managing product licenses

This chapter includes the following topics:

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. After you install Symantec Endpoint Protection Manager, you have 60 days to purchase enough license seats to cover all of your deployed clients.

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. 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 clients that you need to protect the endpoints at your site.

See "About administrator accounts and access rights" on page 281.

Table 5-1 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 and spyware definitions and other security content from LiveUpdate. See "Symantec Endpoint Protection product license requirements" on page 80. See "How many Symantec Endpoint Protection licenses do I need?" on page 101. See "About multi-year licenses" on page 103.
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 trial license expired. ■ Your paid license expired. ■ Your license is over-deployed. After you purchase your license, you receive an email with a Symantec license file (.slf) or a license serial number. You can use the serial number to activate the installation. You can also use the serial number to download a copy of the .slf file from MySymantec. You do not need to manually download a license file. See "About purchasing Symantec Endpoint Protection licenses" on page 97. See "Checking the license status in Symantec Endpoint Protection Manager" on page 100. See "About the trial license" on page 96. See "About managing your licenses" on page 99.

Table 5-1 Licensing tasks *(continued)*

Task	Description
Activate your purchased license	You use the License Activation Wizard in the Symantec Endpoint Protection Manager console to import and activate your Symantec product license. Before you activate the license, you must have one of the following items: ■ 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 product license" on page 51. See "About managing your licenses" on page 99.
Back up your license files	Back up your license files to preserve them in case the database or the computer's hard disk becomes damaged. See "Backing up your license files" on page 102. See "Recovering a deleted license" on page 102.
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 663.
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 the license status in Symantec Endpoint Protection Manager" on page 100. See "About renewing your Symantec Endpoint Protection license" on page 99.

About the trial license

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

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

- Symantec Endpoint Protection Manager
- The Symantec Endpoint Protection client
- Access to LiveUpdate content

After the trial 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 trial license expires 60 days after you install Symantec Endpoint Protection Manager.

See "About purchasing Symantec Endpoint Protection licenses" on page 97.

About purchasing Symantec Endpoint Protection licenses

You need to purchase a license in the following situations:

- Your trial license expired. Symantec Endpoint Protection comes with a trial 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 clients than your current license allows.

Depending upon how you purchase your license, you receive by email either a product license serial number or a Symantec License file. 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 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. However, you may copy and store the license as desired.

Table 5-2 Purchasing license tasks

Task	Description
Determine your licensing requirements	See "Symantec Endpoint Protection product license requirements" on page 80. See "How many Symantec Endpoint Protection licenses do I need?" on page 101.

Table 5-2 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 https://www.symantec.com/partners ■ The Symantec sales team: Visit the Symantec Ordering website for sales contact information.
Learn more about upgrading from the trial license that comes with Symantec Endpoint Protection	See "About the trial license" on page 96.
Get help with purchasing licenses or learn more about licenses	https://support.symantec.com

See "Licensing Symantec Endpoint Protection" on page 94.

Required licensing contact information

The activation process prompts you 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 5-3 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.
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 check box 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 94.

About managing your licenses

You can use MySymantec to download and activate product license keys. However, you can activate licenses from Symantec Endpoint Protection Manager, which is simpler and faster.

The Symantec Licensing Portal is now part of MySymantec. If you have existing credentials for MySymantec, you can use those credentials to access licensing information through the My Products tab.

If you do not have a MySymantec account, you must create one to access license management. The following website provides detailed directions for setting up access to MySymantec:

Getting Started: Everything you need to hit the ground running

See “Activating or importing your Symantec Endpoint Protection product license” on page 51.

See “Licensing Symantec Endpoint Protection” on page 94.

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.

In some cases, you may not receive the notification email and missed any important information that is required to activate your new upgrade. For more information about licensing and product upgrades, see the section pertaining to on-premises software upgrades on the Upgrading Products page.

Symantec Endpoint Protection Manager context-sensitive Help provides additional assistance about the application of an upgrade license specific to the version of Symantec Endpoint Protection that you use.

See “Upgrading to a new release” on page 141.

See “Licensing Symantec Endpoint Protection” on page 94.

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 Symantec Endpoint Protection licenses" on page 97.

See "Activating or importing your Symantec Endpoint Protection product license" on page 51.

See "Recovering a deleted license" on page 102.

Checking the license status in Symantec Endpoint Protection Manager

You can find out whether the management server uses a trial 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 trial license status only provides limited information that is related to the expiration date.

To check whether you have a paid license or trial license

- In the console, do one of the following tasks:
  - Click **Admin** > **Licenses**.
  - Click **Home** > **Licensing Details**.

To check the license expiration date

- In the console, click **Admin** > **Licenses**.

See "Licensing Symantec Endpoint Protection" on page 94.

See "Activating or importing your Symantec Endpoint Protection product license" on page 51.

How many Symantec Endpoint Protection licenses do I need?

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

Table 5-4 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.
Symantec Endpoint Protection components	A Symantec Endpoint Protection license applies to the Symantec Endpoint Protection clients. For instance, in a network with 50 computers, the license must provide for a minimum of 50 seats. Instances of Symantec Endpoint Protection Manager do not require a license. Symantec Endpoint Protection Manager does not require that the client has a license to access the management server. An unlicensed client that connects to the management server is given a license. You must ensure that you have purchased enough license seats to cover each client computer.
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.
Platforms	License seats apply to clients running on any platform, whether the platform is Windows, Mac, or Linux.
Products and versions	License seats apply equally across product versions.

For information on licensing the clients that access the third-party server software, such as Microsoft SQL Server, contact the software vendor.

See “Licensing Symantec Endpoint Protection” on page 94.

See “Purging obsolete non-persistent VDI clients to free up licenses” on page 696.

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 default location: C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\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 website.

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 product license" on page 51.

See "About managing your licenses" on page 99.

See "Licensing Symantec Endpoint Protection" on page 94.

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 the **License recovery** panel, check the box next to 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.

If your license reports show more seats are licensed than known to be deployed, you should purge the database of obsolete clients. Obsolete clients count against the product license, so it is important to purge obsolete clients as soon as they are created. By default, purging occurs every 30 days. You can 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 to make more licenses available

1. In the console, on the **Admin** page, click **Domains**, right-click the domain, and click **Edit Domain Properties**.
2. On the **General** tab, change the **Delete clients that have not connected for specified time** setting from the default of **30** 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.
3. Click **OK**.
4. Wait 24 hours and then revert the settings to 30 days or to another interval that suits your requirements.

See "Purging obsolete non-persistent VDI clients to free up licenses" on page 696.

See "Licensing Symantec Endpoint Protection" on page 94.

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. 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 for you to activate fewer than the full complement of license files. In this case, 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 you activate the third file at a later date, Symantec Endpoint Protection Manager accurately reports the full duration of the license as three years. In all cases, the number of seats remains consistent with the number of seats that you purchased.

When Symantec Endpoint Protection Manager merges files, it deletes the shortest duration files and keeps the longest duration file for internal license-keeping functions. If you think that Symantec Endpoint Protection Manager inappropriately deleted a license, 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 102.

See "Licensing Symantec Endpoint Protection" on page 94.

Licensing an unmanaged Windows client

No unmanaged clients require the manual installation of a license file. However, to enable the submission of reputation data from an unmanaged Windows client, you must install a paid license on the unmanaged client. Unmanaged Mac clients and Linux clients do not submit reputation data.

To license an unmanaged Windows 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. By default, the folder in which the inbox appears is hidden, so use Folder Options to enable the showing of hidden files and folders.

   - On the clients that use Vista or a later version of Windows, the inbox is located by default at C:\ProgramData\Symantec\Symantec Endpoint Protection\CurrentVersion\inbox\
   - On the clients that run 12.1.x on a pre-Vista version of Windows, the inbox is located by default at C:\Documents and Settings\All Users\Application Data\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 Vista or a later version of Windows: C:\ProgramData\Symantec\Symantec Endpoint Protection\CurrentVersion\Data\Config

- For the clients that run 12.1.x on a pre-Vista version of Windows: C:\Documents and Settings\All Users\Application Data\Symantec\Symantec Endpoint Protection\CurrentVersion\Data\Config

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

See "Understanding server data collection and client submissions and their importance to the security of your network" on page 486.

Chapter 6

Managing the client installation

This chapter includes the following topics:

- Windows client installation package and content update sizes

Preparing for client installation

You must install a Symantec Endpoint Protection client on every computer you want to protect, whether the computer is physical or virtual.

Table 6-1 Client computer installation tasks

Action	Description
Identify client computers	Identify the computers on which you want to install the client software. Check that all the computers run a supported operating system. **Note:** Symantec recommends that you also install the client on the computer that hosts Symantec Endpoint Protection Manager. For the most current system requirements, see: Release notes, new fixes, and system requirements for all versions of Endpoint Protection
Identify computer groups (optional)	Identify the computer groups to which you want the clients to belong. For example, you can group clients based on type of computer, to conform to your corporate organization, or to the security level required. You can create these groups before or after you install the client software. You can also import an existing group structure such as an Active Directory structure. See "Managing groups of clients" on page 234. See "Importing existing groups and computers from an Active Directory or an LDAP server" on page 237.
Prepare client computers for deployment and installation	If your users do not have administrative rights for their computers, then you should 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 "Installing Symantec Endpoint Protection clients with Remote Push" on page 60. Prepare the computers for remote client deployment and for successful communication with Symantec Endpoint Protection Manager after installation. See "Preparing Windows and Mac computers for remote deployment" on page 108.

Table 6-1 Client computer installation tasks *(continued)*

Action	Description
Determine features and deploy client software	You deploy the client software using one of the available methods. You can also export a customized client package to deploy later or with a third-party tool. **Note:** Symantec recommends that you do not perform third-party installations simultaneous to the installation of Symantec Endpoint Protection. The installation of any third-party programs that make network- or system-level changes may cause undesirable results when you install Symantec Endpoint Protection. If possible, restart the client computers before you install Symantec Endpoint Protection. See "Choosing a method to install the client using the Client Deployment Wizard" on page 119. See "Exporting client installation packages" on page 136. See "Installing Windows client software using third-party tools" on page 812. ■ You decide which features to install to the client computers. You configure custom client feature sets and installation settings before you export or deploy an installation package. Installation settings include the installation folder and the restart settings. You can also use the default client install feature sets and installation settings. See "Choosing which security features to install on the client" on page 121. See "About the Windows client installation settings" on page 123. See "Choosing which security features to install on the client" on page 121. ■ For Windows clients, you can choose to automatically uninstall existing third-party security software when you configure client installation settings. See "Configuring client packages to uninstall existing security software" on page 124.
Verify installation status	Confirm that the client installation succeeded and that clients communicate with Symantec Endpoint Protection Manager. Managed clients may not appear in the console until after they are restarted. See "Symantec Endpoint Protection client status icons" on page 165. See "Restarting the client computers from Symantec Endpoint Protection Manager" on page 127.

After installation, you can take additional steps to secure unmanaged computers and optimize the performance of your Symantec Endpoint Protection installation.

See "Getting up and running on Symantec Endpoint Protection for the first time" on page 36.

Preparing Windows and Mac computers for remote deployment

Before you deploy Symantec Endpoint Protection from Symantec Endpoint Protection Manager, you must take steps to prepare the computers to ensure a successful remote installation.

These steps pertain only to remote installation. You can reverse these changes afterward, but you must apply them again to perform another remote installation.

Table 6-2 lists the tasks that you must perform on all computers to which you plan to remotely deploy the Symantec Endpoint Protection client.

Table 6-3 lists the additional tasks that you must perform on Windows computers. See your Windows documentation for more information on any tasks you do not know how to perform.

Table 6-4 lists the additional tasks that you must do on Mac computers. See your Mac documentation for more information on any tasks you do not know how to perform.

Note: You cannot deploy the Symantec Endpoint Protection client to Linux computers remotely from Symantec Endpoint Protection Manager.

Table 6-2 Tasks to prepare all computers for remote deployment

Task	Details
Have administrative rights to your client computers	If the client computer is part of an Active Directory domain, you should use domain administrator account credentials for a remote push installation. Otherwise, have the administrator credentials available for each computer to which you deploy.
Modify firewall settings	Modify firewall settings to allow communication between Symantec Endpoint Protection components. See "Communication ports for Symantec Endpoint Protection" on page 112.
Uninstall existing third-party security software	Uninstall any third-party security software currently in use. For Windows computers, Symantec Endpoint Protection version 12.1 RU1 MP1 and later includes a tool to help automatically uninstall select third-party security software. You must separately uninstall any security software that this tool does not uninstall. **Note:** Some programs may have special uninstallation routines, or may need to have a self-protection component disabled. See the documentation for the third-party software. You configure this tool before you deploy, and the uninstallation occurs before Symantec Endpoint Protection installs. See "Configuring client packages to uninstall existing security software" on page 124.
Uninstall Symantec Endpoint Protection clients that do not uninstall normally	As of 14, you can uninstall an existing installation of the Symantec Endpoint Protection client for Windows. You should only use this option if the existing Symantec Endpoint Protection installation does not uninstall normally. You should not use this option as part of a standard deployment. You configure this tool before you deploy, and the uninstallation occurs before Symantec Endpoint Protection installs. See "Configuring client packages to uninstall existing security software" on page 124.

Table 6-2 Tasks to prepare all computers for remote deployment *(continued)*

Task	Details
Uninstall unsupported or consumer Symantec security software	Uninstall any unsupported Symantec security software, such as Symantec AntiVirus or Symantec Client Security. Migration directly from these products is not supported. You must also uninstall any consumer-branded Symantec security products, such as Norton Internet Security. See the documentation for your Symantec software for information about uninstallation. See "Supported upgrade paths to the latest version of Symantec Endpoint Protection 14.x" on page 144.

Table 6-3 Windows remote deployment preparation tasks

Operating system	Tasks
Prepare Windows Vista, Windows 7, or Windows Server 2008 / 2008 R2 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. To disable UAC remote restrictions, see: http://support.microsoft.com/kb/951016 Perform the following tasks: ■ Disable the Sharing Wizard. The Sharing Wizard prevents more advanced sharing options from working during Remote Push. ■ Enable network discovery by using the Network and Sharing Center. Network discovery lets you browse the network. You do not need it to search the network. ■ Enable the built-in administrator account and assign a password to the account. Remote Push fails when the local administrator account has a blank password. If the Windows client computer is part of an Active Directory domain, use domain administrator account credentials with local administrator privileges for Remote Push. ■ Verify that the account with which you push the installation has administrator privileges. ■ Enable and start the Remote Registry service. ■ Disable or remove Windows Defender. Consult the operating system's documentation for guidance on how to successfully complete these tasks.

Table 6-3 Windows remote deployment preparation tasks *(continued)*

Operating system	Tasks
Prepare Windows 8 / 8.1 or later, or Windows Server 2012 / 2012 R2 or later computers	Before you deploy, perform the following tasks: ■ Disable the registry key LocalAccountTokenFilterPolicy. To disable UAC remote restrictions, see: http://support.microsoft.com/kb/951016 ■ Enable and start the Remote Registry service. ■ Disable or remove Windows Defender.

Table 6-4 Mac remote deployment preparation tasks

Operating system	Tasks
Prepare the Mac computers on any supported operating system	Before you deploy, perform the following tasks on the Mac computers: ■ Click **System Preferences > Sharing > Remote Login** and either allow access for all users, or only for specific users, such as Administrators. ■ If you use the Mac firewall, disable stealth mode. With stealth mode enabled, the remote push installation cannot discover the client through **Search Network**. To disable stealth mode on the Mac, see the following article that applies to your version of the Mac operating system. macOS High Sierra: Prevent others from discovering your Mac (10.13; Symantec Endpoint Protection 14.0.1) macOS Sierra: Prevent others from discovering your Mac (10.12; Symantec Endpoint Protection 12.1.6 MP6 - 14.0.1) OS X El Capitan: Prevent others from discovering your Mac (10.11; Symantec Endpoint Protection 12.1.6 MP2 - 14.0.1) OS X Yosemite: Prevent others from discovering your Mac (10.10; Symantec Endpoint Protection 12.1.5 - 14.0.1) ■ Ensure that the firewall does not block the port that Secure Shell (SSH) uses. By default, this port is TCP port 22. This port allows the required communication for remote logon. ■ The Bonjour service does not support IPv6 networking. To ensure that **Browse Network** or **Search Network** displays these Macs, ensure that they also have IPv4 networking enabled.

See "Communication ports for Symantec Endpoint Protection" on page 112.

See "Installing Symantec Endpoint Protection clients with Remote Push" on page 60.

See "Preparing for client installation" on page 107.

Communication ports for Symantec Endpoint Protection

If the computers that run Symantec Endpoint Protection Manager and the Symantec Endpoint Protection client also run third-party firewall software or hardware, you must open certain ports. These ports are for remote deployment and for communication between the management server and clients. See your firewall product documentation for instructions to open ports or allow applications to use ports.

By default, the firewall component of Symantec Endpoint Protection already allows traffic on these ports.

Warning: The firewall in the Symantec Endpoint Protection client is disabled by default at initial installation until the computer restarts. 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 6-5 Ports for client and server installation and communication

Protocol and port number	Used for	Listening process	Description	Applicable versions
TCP 139, 445 UDP 137, 138	Push deployment from Symantec Endpoint Protection Manager to Windows computers	svchost.exe	■ Initiated by Symantec Endpoint Protection Manager (clientremote.exe) ■ Not configurable Also uses TCP ephemeral ports.	All
TCP 22	Push deployment from Symantec Endpoint Protection Manager to Mac computers	launchd	■ Initiated by Symantec Endpoint Protection Manager (clientremote.exe) ■ Not configurable	All
TCP 2967	Group Update Provider (GUP) web-caching proxy functionality	ccSvcHst.exe	■ Initiated by Symantec Endpoint Protection clients ■ Configurable	All
TCP 2968	WSS Traffic Redirection Client Authentication	ccSvcHst.exe	■ Initiated by Symantec Endpoint Protection clients ■ Configurable	As of 14.2

Table 6-5 Ports for client and server installation and communication *(continued)*

Protocol and port number	Used for	Listening process	Description	Applicable versions
TCP 2638	Communication between the embedded database and Symantec Endpoint Protection Manager	dbsrv16.exe	■ Initiated by Symantec Endpoint Protection Manager ■ Configurable	All
TCP 1433	Communication between a remote SQL Server database and Symantec Endpoint Protection Manager	sqlserver.exe	■ Initiated by Symantec Endpoint Protection Manager ■ Configurable The Symantec Endpoint Protection Manager management server also uses TCP ephemeral ports.	All
TCP 8443	Server communication (HTTPS)	SemSvc.exe	All logon information and administrative communication takes place using this secure port. ■ Initiated by the Java-based remote console or web-based remote console, or by replication partners ■ Configurable Symantec Endpoint Protection Manager listens on this port.	All

Table 6-5 Ports for client and server installation and communication *(continued)*

Protocol and port number	Used for	Listening process	Description	Applicable versions
TCP 9090	Web console communication	SemSvc.exe	This port is used only for initial HTTP communication between the remote management console and Symantec Endpoint Protection Manager. This initial communication includes installation, and to display the logon screen only. ■ Initiated by the remote Web console ■ Configurable Also uses TCP ephemeral ports.	All
TCP 8014	Communication between Symantec Endpoint Protection Manager (HTTP) and the Symantec Endpoint Protection client	httpd.exe (Apache)	■ Initiated by Symantec Endpoint Protection clients ■ Configurable Clients also use TCP ephemeral ports.	All
TCP 443	Communication between the Symantec Endpoint Protection Manager (HTTPS) and the Symantec Endpoint Protection client	httpd.exe (Apache)	■ Initiated by Symantec Endpoint Protection clients ■ Configurable Clients also use TCP ephemeral ports.	All

Table 6-5 Ports for client and server installation and communication *(continued)*

Protocol and port number	Used for	Listening process	Description	Applicable versions
TCP 443	Communication between the Symantec Endpoint Protection Manager and the cloud console	prunsvr.exe	For information on which domains to add to the proxy bypass list for the cloud console, see: Proxy error messages appear in the Endpoint Protection Manager Cloud tab > Troubleshooting	As of 14.0.1
HTTPS 443	Communication between the Symantec Endpoint Protection roaming client and the cloud console	None	Managed clients that have intermittent communication with Symantec Endpoint Protection Manager upload their critical events directly to the cloud console. Symantec Endpoint Protection Manager must be enrolled with the cloud console. See "Monitoring roaming Symantec Endpoint Protection clients from the cloud console" on page 276.	As of 14.2
HTTP 8081 HTTPS 8082	Communication between Symantec Endpoint Protection Manager and the Content Analysis server appliance	Symantec Endpoint Protection Manager	The management server uses this port to communicate with the Content Analysis server or the Malware Analysis Appliance.	As of 14.2
TCP 8445	Used by the remote reporting console	httpd.exe (Apache)	■ Initiated by the reporting console ■ Configurable	All

Table 6-5 Ports for client and server installation and communication *(continued)*

Protocol and port number	Used for	Listening process	Description	Applicable versions
TCP 8446	Web services	semapisrv.exe	Remote management applications use this port to send web services traffic over HTTPS. ■ Initiated by Remote Monitoring and Management (RMM) and by EDR ■ Configurable ■ Used for Java Remote Console (as of version 14.0.1)	All
TCP 8447	Process launcher	semlaunchsrv.exe	This virtual service account launches any Symantec Endpoint Protection Manager processes that require higher privileges, so that these other services do not need to have them. Only honors requests from localhost. ■ Initiated by Symantec Endpoint Protection Manager (SemSvc.exe) ■ Configurable	All, as of 12.1.5

Table 6-5 Ports for client and server installation and communication *(continued)*

Protocol and port number	Used for	Listening process	Description	Applicable versions
TCP 8765	Server control	SemSvc.exe	Used by Symantec Endpoint Protection Manager for Tomcat web service for shutdown. ■ Initiated by Symantec Endpoint Protection Manager ■ Configurable	All
TCP 1100	Remote object registry	SemSvc.exe	Tells AjaxSwing on which port to run RMI Registry. ■ Initiated by AjaxSwing ■ Not configurable	All
UDP 514	Forwarding data to a Syslog server (Optional)	SemSvc.exe	■ Outbound traffic from Syslog server to Symantec Endpoint Protection Manager ■ Inbound traffic to Syslog server ■ Configurable Traffic to or from Symantec Endpoint Protection Manager uses UDP ephemeral ports.	

- Windows Vista and later 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 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 “About basic management server settings” on page 86.

See “Preparing Windows and Mac computers for remote deployment” on page 108.

See “Monitoring endpoint protection” on page 625.

See “Preparing for client installation” on page 107.

How to choose a client installation type

Choose the client type for the client installation package.

Version 14.x includes cloud-enabled options for Windows client installation packages. These options replace 12.1.x standard-size and reduced-size client installation packages. The cloud-enabled options include a standard client and an embedded/VDI client. Symantec Endpoint Protection also includes a dark network installation for clients that are not connected to the cloud.

Standard client (as of 14)

- Uses virus and spyware definitions in the cloud.
- Installs only the latest virus and spyware definitions on disk.

  The standard client is approximately 80 percent to 90 percent smaller on disk than legacy standard or dark network Windows clients.
- Handles AutoUpgrade with deltas rather than full installation.

Dark network client (as of 14)

- Cannot use definitions in the cloud.
- Intended for clients with intermittent or no access to the cloud.
- Installs the full set of virus and spyware definitions.
- Similar to legacy standard-size client; uses reputation lookups for Download Insight and SONAR if connected to the cloud.
- Handles AutoUpgrade with deltas rather than full installation.

Standard client (12.1.x)

- Cannot use virus and spyware definitions in the cloud, but uses reputation lookups for Download Insight and SONAR.
- Installs the full set of virus and spyware definitions.
- Handles AutoUpgrade with deltas rather than full installation.

Embedded/VDI client (as of 14)

- Uses virus and spyware definitions in the cloud.
- Installs only the latest virus and spyware definitions. The client is approximately 80 percent to 90 percent smaller on disk than dark network Windows clients.
- The embedded/VDI client includes more size optimizations than the standard client:
  - The installer cache does not save after installation completes. This change means you cannot remove or modify the installation through the Control Panel unless you first copy the installation package to the client computer.
  - The embedded client employs NTFS compression on more folders than the standard client.
- Handles AutoUpgrade with full installation packages; cannot use deltas.

Embedded/VDI client (as of 12.1.6)

- Cannot use virus and spyware definitions in the cloud.
- Installs only the latest virus and spyware definitions. The legacy client is approximately 80 percent to 90 percent smaller on disk than legacy standard Windows clients.
- This client provides slightly less protection than the 12.1.x standard client. Symantec recommends that you install and enable all protection features, which include the firewall, Download Insight, intrusion prevention, and SONAR. For the highest level of security, use the system lockdown feature.
- Includes the same size optimizations as the newer embedded client.
- Handles AutoUpgrade with full installation packages; cannot use deltas
- Introduced in 12.1.6.

Symantec Endpoint Protection support for Windows Embedded

See "Symantec Endpoint Protection client for Windows Embedded system requirements" on page 75.

See "Choosing a method to install the client using the Client Deployment Wizard" on page 119.

See "Exporting client installation packages" on page 136.

Choosing a method to install the client using the Client Deployment Wizard

After you install Symantec Endpoint Protection Manager, you install the Symantec Endpoint Protection client with the Client Deployment Wizard.

Table 6-6 Client installation methods

Options	Description
Save Package	This installation option creates an executable installation package that you save on the management server and then distribute to the client computers. The users then install the client software, so they must have local administrator rights to their computers. You can install Windows, Mac, and Linux clients using this option. See "Installing Symantec Endpoint Protection clients with Save Package" on page 53.
Remote Push	Remote push installation pushes the client software to the computers that you specify. The installation begins automatically on the client computers. Remote push installation does not require the user to have local administrator rights to their computers. You can install Windows and Mac clients using this option. See "Installing Symantec Endpoint Protection clients with Remote Push" on page 60. See "Preparing Windows and Mac computers for remote deployment" on page 108.
Web Link and Email	Users receive an email message that contains a link to download and install the client software. The users then install the client software, so they must have local administrator rights to their computers. You can install Windows, Mac, and Linux clients using this option. See "Installing Symantec Endpoint Protection clients with Web Link and Email" on page 63.

Before you run the Client Deployment Wizard, you review the installation options, optionally customize them, and then select those options during installation. Installation options include the protection technologies to install, the installation destination folder, and the restart behavior after installation.

See "Choosing which security features to install on the client" on page 121.

See "About the Windows client installation settings" on page 123.

See "Preparing for client installation" on page 107.

Choosing which security features to install on the client

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

After installation, make sure to keep all protections enabled.

Table 6-7 Client installation feature sets (Windows)

Feature set	Description
Full Protection for Clients	Recommended for workstations, desktop, and laptop computers. Includes all protection technologies. Appropriate for laptops, workstations, and desktops. Includes the full download protection and mail protocol protection. Whenever possible, use Full Protection for maximum security.
Full Protection for Servers	Recommended for servers. Includes all protection technologies except email scanner protection. Appropriate for any servers that require maximum network security, including the Symantec Endpoint Protection Manager server.
Basic Protection for Servers	Recommended for high-throughput servers. Includes Virus and Spyware Protection and Basic Download Protection. Since intrusion prevention may cause performance issues on high-throughput servers, this option is appropriate for any servers that require maximum network performance.

The Mac client installation package installs Virus and Spyware Protection and intrusion prevention. You cannot customize the features for the Mac client installation package.

The Linux client installation package only installs Virus and Spyware Protection.

Customizing the feature set

If you want to install a subset of the protections, create a custom feature set. However, Symantec recommends that you install all protections.

You cannot customize the features for the Mac or Linux client installation package.

To create a custom client installation feature set

1. In the console, click **Admin** > **Install Packages**.
2. Click **Client Install Feature Set** > **Add Client Install Feature Set**.
3. In the **Add Client Install Feature Set** dialog box, type a name and description, and check which protections to install on the client.
4. Click **OK**.

See "How Symantec Endpoint Protection technologies protect your computers" on page 28.

See "Choosing a method to install the client using the Client Deployment Wizard" on page 119.

See "Preparing for client installation" on page 107.

Creating custom Windows client installation packages in Symantec Endpoint Protection Manager

You can customize client installation packages for Symantec Endpoint Protection for Windows by configuring the client installation settings and the client feature sets. This customization lets you configure an installation path, the restart behavior after installation, whether the installation package uninstalls a third-party security product, among others.

Note: Client Install Settings and Client Install Feature Set configurations only apply to Windows install packages. You can export a Macintosh or Linux install package through **Admin > Install Packages > Client Install Package**, but the configuration options differ.

Table 6-8 Tasks to create a custom Windows client installation package

Task	Details
Create a new custom client installation settings configuration	Use **Client Install Settings** to define the installation behavior. If you want to uninstall existing security software on your client computers, you configure it here. See "Customizing the client installation settings" on page 124. See "Configuring client packages to uninstall existing security software" on page 124.
Create a new custom feature set	**Client Install Feature Sets** define what protection technologies install on the client computer. See "Choosing which security features to install on the client" on page 121.

Table 6-8 Tasks to create a custom Windows client installation package *(continued)*

Task	Details
Create a new, custom installation package	When you export a client installation package, you select from the customized settings files you created. You also choose to where you save the package, and whether the package is a single file (.EXE) or a folder of files. You can also use the custom installation settings and the custom feature sets with the Client Deployment Wizard. See "Exporting client installation packages" on page 136. See "Installing Symantec Endpoint Protection clients with Remote Push" on page 60.

See "Preparing for client installation" on page 107.

About the Windows client installation settings

The Client Deployment Wizard prompts you to specify the client installation settings for Windows clients. The client installation settings define the options of the installation process itself. You can define the target installation folder, whether to disable installation logging, and the post-installation restart settings, among other options.

You can choose the default client installation settings, or you can add a custom **Client Install Settings** under **Admin > Install Packages > Client Install Settings**. The contextual Help provides details about the settings that you can configure.

You should use silent installations for remote deployment to minimize user disruption. When you use a silent deployment, you must restart the applications that plug into Symantec Endpoint Protection, such as Microsoft Outlook.

If you use unattended installations (**Show progress bar only**), Windows may display to users one or more pop-up windows. However, the installation should not fail even if the user does not notice them.

You should not use an interactive installation for remote deployment. This installation type fails unless the user interacts with it. Security features (such as Windows Session 0 isolation) on some operating systems may cause the interactive installation wizard to not appear. You should only use the interactive installation type for local installations. These recommendations apply to both 32- and 64-bit operating systems.

See "Customizing the client installation settings" on page 124.

See "Choosing which security features to install on the client" on page 121.

See "Installing Symantec Endpoint Protection clients with Remote Push" on page 60.

See "How Symantec Endpoint Protection technologies protect your computers" on page 28.

See "Preparing for client installation" on page 107.

Customizing the client installation settings

You can change the installation settings that you apply to a client installation package and for AutoUpgrade.

For example, if you want to install the client to a custom installation folder, or reset the client-server communication settings, you create custom client installation settings. You then apply this custom setting when you export or deploy a package, or set up AutoUpgrade.

To customize the client installation settings

1. In the console, click **Admin > Install Packages > Client Install Settings**.
2. Under **Tasks**, click **Add Client Install Settings**.

   The default client install settings files cannot be modified.
3. Choose the operating system for which the setting file applies.
4. Enter a name and a description.
5. Make your selections from the available options on these tabs:
   - Windows: **Basic Settings** and **Restart Settings**
   - Mac: **Restart Settings** and **Upgrade Settings**

   Note: Mac client restart and upgrade settings apply only to AutoUpgrade.

   For detailed information on these options, click **Help**.
6. Click **OK** to save these settings.

When you run the Client Deployment Wizard or configure AutoUpgrade, select the settings that you created from the drop-down menu next to **Install Settings**.

See "About the Windows client installation settings" on page 123.

See "Configuring client packages to uninstall existing security software" on page 124.

Configuring client packages to uninstall existing security software

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

You enable the security software removal feature by creating or modifying a custom client installation settings configuration. You then select this custom configuration during deployment.

You can use this feature to uninstall third-party security software. To see which third-party software the client package removes, see: Third-party security software removal support in Symantec Endpoint Protection. Some programs may have special uninstallation routines, or may need to have a self-protection component disabled. See the documentation for the third-party software.

You cannot remove third-party security software with Mac or Linux client packages. You can remove third-party security software with Windows client packages as of version 12.1.1 MP1. You must uninstall third-party security software before you deploy the Symantec Endpoint Protection client package.

Note: Changes to the third-party security software removal for version 14.2 mean that you cannot enable it for installation packages for earlier versions. For example, you cannot enable third-party security software removal for version 14.0.1 client packages if you create them with and deploy them from Symantec Endpoint Protection Manager version 14.2.

As of 14, you can also remove existing installations of Symantec Endpoint Protection that you cannot uninstall through standard methods, such as Windows Control Panel. This feature appears as a separate option in the client installation settings.

Only the packages you create using the following procedure can remove existing security software.

To configure client packages to uninstall existing 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 installation 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, click one of the following:
   - **Automatically uninstall existing third-party security software**
     To see which third-party software the client package removes, see Third-party security software removal in Endpoint Protection.
   - **Remove existing Symantec Endpoint Protection client software that cannot be uninstalled**

See "About the Symantec Endpoint Protection client preinstall removal feature" on page 126.

4 Read the information about the option you chose, and then click **OK**.

You can also modify other options for this configuration. Click **Help** for more information about these options.

5 Click **OK** to save the configuration.

To deploy client packages to uninstall existing security software

1 In the console, on the **Home** page, launch the **Client Deployment Wizard**.

Click **Help > Getting Started Page** and then under **Required tasks**, click **Install the client software on your computers**.

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

You can use **Existing Package Deployment** to deploy install packages you previously created. However, you must have exported these packages using a custom client installation settings configuration like the one described in the previous procedure.

3 In **Select Group and Install Feature Set**, select a Windows install package. In the **Install Settings** drop-down list, select the custom client installation settings configuration that you created or modified in the previous procedure. Click **Next**.

4 Click the deployment method that you want to use, and then click **Next** to proceed with and complete your chosen deployment method.

See "Choosing a method to install the client using the Client Deployment Wizard" on page 119.

See "About the Windows client installation settings" on page 123.

See "Preparing for client installation" on page 107.

About the Symantec Endpoint Protection client preinstall removal feature

As of 14, you can uninstall the existing client installation on the client computer before the installation of Symantec Endpoint Protection begins. This feature is comparable to the CleanWipe utility, so you should not enable it for all deployments. Instead, you should only use this feature to remove corrupted or malfunctioning installations of the Symantec Endpoint Protection client.

Before you use this feature, be aware of this important information:

- This feature can remove all Symantec Endpoint Protection versions up to and including the version of the installation package you create.

It also removes all versions of Symantec Network Access Control, and the unsupported products Symantec Endpoint Protection 11.x, Symantec AntiVirus 10.x, and Symantec Client Security 3.x.

- Although this feature removes versions earlier than 14, you cannot enable it when you create an installation package for an earlier version. For example, you cannot create a package for version 12.1.6 MP4 that enables this feature.
- This feature cannot uninstall a version of Symantec Endpoint Protection that is later than the installation package with which you include it. For example, you cannot use this feature during a planned rollback.
- If you deploy the wrong package type with this feature enabled, it does not perform the removal. For example, if you deploy a 32-bit package to a 64-bit computer, it cannot install. Therefore, it does not remove the existing Symantec Endpoint Protection installation.
- You cannot use this feature with an installation that uses the .MSI file directly, such as through a GPO deployment.
- This feature does not work with AutoUpgrade.
- This feature does not remove Symantec Endpoint Protection Manager.
- This option only removes Windows LiveUpdate if no other Symantec products use it.
- On the client computer, this feature runs silently, and does not display a status screen or user interface.
- This option forces the installation type to **Silent**.
- The computer restarts automatically after the removal completes. You cannot configure this restart to be postponed or skipped.

See “Configuring client packages to uninstall existing security software” on page 124.

Restarting the client computers from Symantec Endpoint Protection Manager

You need to restart the Windows client computers after you install the client software. By default, the Windows client computers restart automatically after installation, though the user can delay it until a pre-scheduled time overnight. Before you export or deploy the installation package, you can configure the Windows client installation settings to customize the restart after installation. You can configure the restart options on a group to control how the client computers restart after a risk remediation or a new client download.

Mac client computers prompt for a restart after installation. If you push the client package and no one is logged on to the Mac computer, a hard restart occurs automatically when the installation completes. You cannot customize this setting.

Linux client computers do not require a restart and do not automatically restart after installation.

You can also restart the Mac and Windows client computers at any time by running a restart command from the management server. You cannot restart the Linux client with a restart command from the management server. You have the option to schedule the Windows 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. When you send a restart command to a Mac client computer, it always performs a hard restart.

To configure risk remediation and new client download restart options on Windows 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. The default message tells the user that a security risk remediation or a new content download requires a restart.
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 the Windows client installation settings” on page 123.

See “What are the commands that you can run on client computers?” on page 250.

See “Running commands on client computers from the console” on page 253.

See “Preparing for client installation” on page 107.

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. Install an unmanaged client so that the user has more control over the computer, such as a test computer, or if the computer is primarily off-site. 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.

You can convert an unmanaged client to a managed client at a later time by replacing the client-server communications file on the client computer.

Table 6-9 Differences between a managed and an unmanaged client

Type	Description
Managed client	Managed clients connect to the Symantec Endpoint Protection Manager. You administer the client computers from the Symantec Endpoint Protection Manager console. You use the console to update the client software, security policies, and virus definitions on the managed client computers. The managed client can get content updates from Symantec Endpoint Protection Manager, GUPs, the Internet, and LiveUpdate. In most cases, you install the client software as a managed client. You can install a managed client in one of the following ways: ■ During initial product installation ■ From the console after installation

Table 6-9 Differences between a managed and an unmanaged client *(continued)*

Type	Description
Unmanaged client	The primary computer user must administer the client computer. An unmanaged client does not connect to Symantec Endpoint Protection Manager and cannot be administered from the console. In most cases, unmanaged clients connect to your network intermittently or not at all. The primary computer user must update the client software, security policies, and virus definitions on the unmanaged client computer. The unmanaged client can get content updates from the Internet and LiveUpdate. You must update the content on each client individually. See "How to get an unmanaged client installation package" on page 130. See "Installing an unmanaged Windows client" on page 131.

See "How does the client computer and the management server communicate?" on page 168.

See "How do I replace the client-server communications file on the client computer?" on page 171.

See "Preparing for client installation" on page 107.

How to get an unmanaged client installation package

You can get the unmanaged Symantec Endpoint Protection client installation package in one of the following ways:

- Download a standalone installer from MySymantec
  Download the latest version of Symantec Endpoint Protection
- Copy a folder from within the installation file, whether you downloaded it from MySymantec, or received a physical disc.
  The folders SEP (32-bit) or SEPx64 (64-bit) contain the unmanaged Windows client, SEP_MAC contains the unmanaged Mac client, and SEP_LINUX contains the unmanaged Linux client.
- Export an unmanaged client from Symantec Endpoint Protection Manager with the default policies and settings, or with custom policies and settings.
  For custom policy and settings recommendations for unmanaged clients, see Recommended policies and settings for unmanaged client installation packages.
  See "Exporting client installation packages" on page 136.

You cannot export an unmanaged Mac client with group policies.

You copy the client installer package to the client computer for installation. If the file is a .zip file, you must extract all contents before you install.

See “Installing an unmanaged Windows client” on page 131.

See “Installing the Symantec Endpoint Protection client for Mac” on page 55.

See “Installing the Symantec Endpoint Protection client for Linux” on page 58.

See “About managed and unmanaged clients” on page 129.

Installing an unmanaged Windows client

An unmanaged (or self-managed) client usually allows a user greater control of Symantec Endpoint Protection settings through the client user interface. Typically, you install an unmanaged Symantec Endpoint Protection client directly on to a Windows computer, and the installation requires user input to complete.

See “About managed and unmanaged clients” on page 129.

See “How to get an unmanaged client installation package” on page 130.

Note: When you install a managed Windows client installation package directly on to the client computer, the steps to install are similar. Only an **Interactive** installation requires user input. The client installation setting options **Show progress bar only** and **Silent** do not require user input.

To install an unmanaged Windows client

Note: Unmanaged client packages that are configured with custom policies may not display during installation some of the panels that are described. If you do not see an installation panel that the procedure step describes, skip to the next step.

1. Copy the installation file or Symantec Endpoint Protection Manager folder to the client computer, and then double-click `Setup.exe`. Click **Next**.

   If you purchased a physical disc and want to install an unmanaged client, insert the disc. The installation should start automatically. If it does not start automatically, double-click `Setup.exe`. Click **Install an unmanaged client**.

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

3 On the **Setup Type** panel, click one of the following options:

Click **Typical** for the most common options, and then click **Next**.

Click **Custom** to configure your installation, click **Next**, select the protection types, and then click **Next**.

See "Choosing which security features to install on the client" on page 121.

4 If the installation wizard prompts you, click **Enable Auto-Protect** and **Run LiveUpdate**, and then click **Next**

5 On the **File Reputation Data Submission** panel, uncheck the box if you do not want to provide pseudonymous file reputation data to Symantec, and then click **Next**.

An unmanaged client does not submit reputation data without a paid license, even if you leave the box checked.

See "Licensing an unmanaged Windows client" on page 104.

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

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

See "Installing the Symantec Endpoint Protection client for Mac" on page 55.

See "Installing the Symantec Endpoint Protection client for Linux" on page 58.

See "About the Windows client installation settings" on page 123.

See "Preparing for client installation" on page 107.

Uninstalling the Symantec Endpoint Protection client for Windows

You can uninstall the Windows client in the following ways:

- By using the Windows Control Panel to remove an application, typically **Programs and Features**.
- By configuring and deploying a custom client installation package that removes the Symantec Endpoint Protection client (as of 14). Only use this method if uninstalling with the Windows Control Panel does not work.
  See "About the Symantec Endpoint Protection client preinstall removal feature" on page 126.
- For alternative methods to uninstall Symantec Endpoint Protection Manager and other components, see Uninstall Symantec Endpoint Protection.

If the Symantec Endpoint Protection client software uses a policy that blocks hardware devices, the policy blocks the devices after you uninstall the software. If you do not disable the device control by policy before you uninstall, use the Windows Device Manager to unblock the devices.

To uninstall the Symantec Endpoint Protection client for Windows

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 installation 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 **Remove existing Symantec Endpoint Protection client software that cannot be uninstalled**.
4. Read the message, and then click **OK**.
5. Click **OK**.

See "Uninstalling the Symantec Endpoint Protection client for Mac" on page 133.

See "Uninstalling the Symantec Endpoint Protection client for Linux" on page 134.

Uninstalling the Symantec Endpoint Protection client for Mac

You uninstall the Symantec Endpoint Protection client for Mac through the client icon on the menu bar. Uninstallation of the Symantec Endpoint Protection client for Mac requires administrative user credentials.

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

To uninstall the Symantec Endpoint Protection client for Mac

1. On the Mac client computer, open the Symantec Endpoint Protection client, and then click **Symantec Endpoint Protection > Uninstall Symantec Endpoint Protection**.
2. Click **Uninstall** again to begin the uninstallation.

3 When you are prompted, authenticate with your Mac's administrative user name and password.

You may also be prompted to type a password to uninstall the client. This password may be a different password than your Mac's administrative password.

4 Once the uninstallation completes, click **Restart Now**.

If the uninstallation fails, you may have to use an alternate method to uninstall. See:

Uninstall Symantec Endpoint Protection

See "Password-protecting the Symantec Endpoint Protection client" on page 260.

Uninstalling the Symantec Endpoint Protection client for Linux

You uninstall the Symantec Endpoint Protection client for Linux with the script that the installation provides.

Note: You must have superuser privileges to uninstall the Symantec Endpoint Protection client on the Linux computer. The procedure uses `sudo` to demonstrate this elevation of privilege.

To uninstall the Symantec Endpoint Protection client for Linux

1 On the Linux computer, open a terminal application window.

2 Navigate to the Symantec Endpoint Protection installation folder with the following command:

```
cd /opt/Symantec/symantec_antivirus
```

The path is the default installation path.

3 Use the built-in script to uninstall Symantec Endpoint Protection with the following command:

```
sudo ./uninstall.sh
```

Enter your password if prompted.

This script initiates the uninstallation of the Symantec Endpoint Protection components.

4 At the prompt, type **Y** and then press **Enter**.

Uninstallation completes when the command prompt returns.

Note: On some operating systems, if the only contents of the `/opt` folder are the Symantec Endpoint Protection client files, the uninstaller script also deletes `/opt`. To recreate this folder, enter the following command: `sudo mkdir /opt`

To uninstall using a package manager or software manager, see the documentation specific to your Linux distribution.

Managing client installation packages

To manage clients with Symantec Endpoint Protection Manager, you must export a managed client installation package, and then install the package files onto client computers. You can deploy the client with either Symantec Endpoint Protection Manager or a third-party deployment tool.

Symantec occasionally provides updated packages of installation files, usually when a new product version releases. You can automatically update the client software on all managed Windows and Mac clients in a group with the AutoUpgrade feature. You do not need to redeploy software with installation deployment tools.

Table 6-10 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 "Choosing which security features to install on the client" on page 121. See "About the Windows client installation settings" on page 123.

Table 6-10 Client installation package-related tasks *(continued)*

Task	Description
Export client installation packages	You can export packages for managed clients or unmanaged clients. You can export the 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. See "Exporting client installation packages" on page 136. See "How to get an unmanaged client installation package" on page 130. See "Installing an unmanaged Windows client" on page 131.
Import client installation package updates	You can add updated client installation packages 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 "Importing client installation packages into Symantec Endpoint Protection Manager" on page 138.
Upgrade Windows and Mac 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 Symantec Endpoint Protection Manager and make them available for exporting. However, you do not have to reinstall them with client deployment tools. The easiest way to update Windows and Mac clients with the latest software is to use AutoUpgrade. You should first update a group with a small number of test computers. See "Upgrading client software with AutoUpgrade" on page 156. You can also update clients with LiveUpdate if you permit clients to run LiveUpdate and if the LiveUpdate Settings policy permits updates.
Delete client installation packages	You can delete older client installation packages to save disk space. However, AutoUpgrade sometimes uses the older Windows client installation packages to build upgrade packages. The upgrade packages result in smaller downloads by clients.

See "Preparing for client installation" on page 107.

Exporting client installation packages

You might want to export a client install package if you need those options that are not available when you use **Save Package** in the **Client Deployment Wizard**. For example, you may need to create an unmanaged client with custom policies. You may also only need either 32-bit or

64-bit installation packages for Windows, or need either DPKG or RPM installation packages for Linux.

Once you export the client install package, you deploy it. **Remote Push** in the **Client Deployment Wizard** can deploy the Windows and Mac packages that you export. Alternately, you can install an exported package directly on to the client, or use a third-party program to deploy it.

You can 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 Windows or Mac 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 the clients do not appear in the correct domain groups.

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 you want to export and then click **Export**.
4. Click **Browse** to navigate to and select the folder to contain the exported package, and then click **OK**.

   Note: Export Package does not support directories with double-byte or high-ASCII characters, and blocks their selection.

   ---

5. Set the other options according to your installation goals. The options vary depending on the type and the platform of the installation package you export.

   For details about the export options in this dialog box, click **Help**.

6. Click **OK**.

See "Importing client installation packages into Symantec Endpoint Protection Manager" on page 138.

See "Choosing which security features to install on the client" on page 121.

See "Installing Symantec Endpoint Protection clients with Save Package" on page 53.

See "Installing Symantec Endpoint Protection clients with Remote Push" on page 60.

See "Restoring client-server communications with Communication Update Package Deployment" on page 173.

See "Preparing for client installation" on page 107.

Importing client installation packages into Symantec Endpoint Protection Manager

You may need to import a client installation package into Symantec Endpoint Protection Manager if:

You upgrade to a newer version of Symantec Endpoint Protection Manager using a database that you have restored from a previous version. The database includes older client installation packages, and you need to import the newer packages.

You should always keep the Symantec Endpoint Protection Manager version the same or later than the client version.

Note: You can import an executable package such as .exe or .zip file packages directly, but it is not recommended. The .info file contains the information that describes the package and ensures proper migration to future builds of the Symantec Endpoint Protection client through delta updates. On the other hand, the Symantec Endpoint Protection Manager web console does not import the .info file format. In the web console, you can only import or export packages in a single file, such as in the .zip or .exe file format.

To import client installation packages into Symantec Endpoint Protection Manager

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

   The client installation package consists of two files. One file is named *product_name*.dat, and the other file is named *product_name*.info. These files automatically import during the installation or upgrade of Symantec Endpoint Protection Manager. You can also get the packages from the `SEPM/Packages` folder of the installation file.

2. In the console, click **Admin** > **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 you copied in step 1, and then click **Select**.

7 When the **Completed successfully** prompt appears, click **Close**.

To export the installation files and make them available for deployment, click **Export this Package**, and then complete this procedure.

See "Exporting client installation packages" on page 136.

After you successfully import the package, you can see a "Package is created" event in the System > Administrative log. The event is described with text similar to "Successfully imported the SEP 12.1 RU5 32-bit package by Symantec Endpoint Protection Manager. This package is now available for deployment."

See "Viewing logs" on page 655.

See "Preparing for client installation" on page 107.

Windows client installation package and content update sizes

Client installation packages, product patches, and content updates are also stored in the Symantec Endpoint Protection database and affect the storage requirements. Product patches contain information for client packages and information for each language or locale. Note that patches also create new, full client builds.

Table 6-11 displays the size of the client installation package if the maximum level of client logging and protection technologies are enabled.

Table 6-11 Windows client installation package size

Client type/Definition type	*Installed with virus definitions?	64-bit package (MB)	32-bit package (MB)
Standard and Embedded (14)	Yes	188	175
CoreDefs-3**	No	93	81
Dark network (14)	Yes	288	276
CoreDefs-1.5	No	93	80
Standard (12.1.6)	Yes	335	316
CoreDefs-1	No	86	70

Table 6-11 Windows client installation package size *(continued)*

Client type/Definition type	*Installed with virus definitions?	64-bit package (MB)	32-bit package (MB)
Reduced (Embedded/VDI) (12.1.6) CoreDefs-3	Yes	182	165
	No	86	70

For these packages, you can set a larger heartbeat. These sizes do not include packet-level firewall logs, which are not recommended in a production environment. If client logging is disabled, and there are no new policies or content to download from the management server, the client installation package is smaller. In this case, you can set a smaller heartbeat.

* If your network has low bandwidth, install the client package without the virus definitions. As soon as the client connects to the management server, the client receives the full set of virus definitions.

All client installation packages include all features, such as Virus and Spyware, the firewall, the IPS, SONAR, System Lockdown, Application Control, Host Integrity content, and so forth. The difference between the client types are the size of the virus and spyware definitions.

See "How to choose a client installation type" on page 118.

In 12.1.5 and later, content updates require less storage space in the database and on the file system. Instead of storing multiple full revisions, the management server now stores only one full content revision plus incremental deltas. In 12.1.6, full content updates require ~470 MB.

Note: As of version 14, you can download security patches to clients the same way as other content, using a LiveUpdate server, the management server, or a Group Update Provider. In 12.1.6 and earlier, security patches are only available as part of new release, and only as part of a client deployment package using AutoUpgrade. See "Downloading Endpoint Protection security patches to Windows clients" on page 230.

Chapter 7

Upgrading Symantec Endpoint Protection

This chapter includes the following topics:

Upgrading to a new release

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. You should also check the known issues that appear in the release notes for any late-breaking information relating to upgrades.

This section is specific to upgrading the software in environments where a compatible version of the product is already installed.

Before you upgrade, review the following information:

- System requirements
  For the most current system requirements, see: Release notes, new fixes, and system requirements for all versions of Endpoint Protection
- New features in this version
  What's new in all versions of Symantec Endpoint Protection
- Upgrade best practices
  See Upgrade best practices for Endpoint Protection 14.x.
- Compatible Symantec Endpoint Protection Manager and Symantec Endpoint Protection client upgrade paths
  See "Supported upgrade paths to the latest version of Symantec Endpoint Protection 14.x" on page 144.

Symantec recommends that you do not perform third-party installations simultaneous to the upgrade of Symantec Endpoint Protection. The installation of any third-party programs that make network- or system-level changes may cause undesirable results when you upgrade Symantec Endpoint Protection. If possible, restart the client computers before you upgrade Symantec Endpoint Protection.

Table 7-1 Process for upgrading Symantec Endpoint Protection

Task	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 754.
Step 2: Break the replication relationship (optional)	If the management server you want to update replicates with other management servers, break the replication relationship. If the second management server, or replication partner, launches replication during the upgrade, it may have unpredictable results. **Note:** Breaking the relationship between the management servers is not the same as removing the replication partner. You do not want to delete the replication partner entirely. See "Disabling replication and restoring replication before and after an upgrade" on page 153.
Step 3: 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 151.

Table 7-1 Process for upgrading Symantec Endpoint Protection *(continued)*

Task	Description
Step 4: Upgrade the Symantec Endpoint Protection Manager software	Install the new version of 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 "Upgrading a management server" on page 149. See "Installing Symantec Endpoint Protection Manager" on page 43.
Step 5: Restore the replication relationship after upgrade (optional)	If the management server you updated replicates with other management servers, restore the replication relationship. See "Disabling replication and restoring replication before and after an upgrade" on page 153.
Step 6: Upgrade Symantec client software	Prepare then upgrade your client software to the latest version. If you use Group Update Providers, they must be upgraded first. See "Choosing which method to upgrade the client software" on page 154. See "Upgrading Group Update Providers" on page 159. See "Preparing for client installation" on page 107. When Symantec provides updates to client installation packages, you add the updates to 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 Windows and Mac 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 client software with AutoUpgrade" on page 156.

See "Logging on to the Symantec Endpoint Protection Manager console" on page 48.

Upgrade resources for Symantec Endpoint Protection

Table 7-2 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 316. See "Symantec Endpoint Protection features based on platform (12.1.x through 14.x)" on page 795. See "About the Windows client installation settings" on page 123. See "Choosing which security features to install on the client" on page 121.
Feature and policy descriptions	See "How Symantec Endpoint Protection technologies protect your computers" on page 28.
Feature dependencies	See "Symantec Endpoint Protection feature dependencies for Windows clients (12.1.x through 14.x)" on page 792.
Manage product licenses	Symantec Endpoint Protection is licensed according to the number of clients that are needed to protect the computers at your site. See "Symantec Endpoint Protection product license requirements" on page 80. See "About product upgrades and licenses" on page 99.
Additional resources	See the following articles: ■ Best practices for upgrading to the latest version of Symantec Endpoint Protection ■ Download the latest version of Symantec Endpoint Protection ■ Release notes, new fixes, and system requirements for all versions of Endpoint Protection

See "Upgrading to a new release" on page 141.

Supported upgrade paths to the latest version of Symantec Endpoint Protection 14.x

Symantec Endpoint Protection Manager and Windows client

The following versions of Symantec Endpoint Protection Manager and Symantec Endpoint Protection Windows client can upgrade directly to 14.2.1:

- 11.x and Small Business Edition 12.0 (Symantec Endpoint Protection clients only, for supported operating systems)
- 12.1.x, up to 12.1.6 MP10 (12.1.7445.7000)
- 14 (14.0.1904.0000)
- 14 MP1 (14.0.2332.0100) or 14 MP1 Refresh Build (14.0.2349.0100)
- 14 MP2 (14.0.2415.0200)
- 14.0.1 (14.0.3752.1000)
- 14.0.1 MP1 (14.0.3876.1100)
- 14.0.1 MP2 (14.0.3929.1200)
- 14.2 (14.2.770.0000)

Note: Valid 14.2 versions 14.2.758.0000 and 14.2.760.0000 were available for a short while with the same component versions. 14.2.770.0000 replaces them.

- 14.2 MP1 (14.2.1023.0100)

Note: Valid 14.2 MP1 version 14.2.1015.0100 was available for a short while with the same component versions. 14.2.1023.0100 replaces it.

Mac client

The following versions of Symantec Endpoint Protection client for Mac can upgrade directly to 14.2.1:

- 12.1.4 - 12.1.6 MP9 (12.1.7369.6900)
  The Mac client did not update for version 12.1.6 MP10.
- 14 (14.0.1904.0000)
- 14 MP1 (14.0.2349.0100 or 14.0.2332.0100)
- 14 MP2 (14.0.2415.0200)
- 14.0.1 (14.0.3752.1000)
- 14.0.1 MP1 (14.0.3876.1100)
- 14.2 (14.2.770.0000)

Note: Valid 14.2 versions 14.2.758.0000 and 14.2.760.0000 were available for a short while with the same component versions. 14.2.770.0000 replaces them.

- 14.2 MP1 (14.2.1023.0100)

  Note: Valid 14.2 MP1 version 14.2.1015.0100 was available for a short while with the same component versions. 14.2.1023.0100 replaces it.

Note: The Symantec Endpoint Protection client for Mac was not updated for 14.0.1 MP2.

Linux client

The following versions of Symantec Endpoint Protection client for Linux can upgrade directly to 14.2.1:

- 12.1.x, up to 12.1.6 MP9 (12.1.7369.6900)
  The Linux client did not update for version 12.1.6 MP10.
- 14 (14.0.1904.0000)
- 14 MP1 (14.0.2349.0100 or 14.0.2332.0100)
- 14 MP2 (14.0.2415.0200)
- 14.0.1 (14.0.3752.1000)
- 14.0.1 MP1 (14.0.3876.1100)
- 14.0.1 MP2 (14.0.3929.1200)
- 14.2 (14.2.770.0000)

  Note: Valid 14.2 versions 14.2.758.0000 and 14.2.760.0000 were available for a short while with the same component versions. 14.2.770.0000 replaces them.

- 14.2 MP1 (14.2.1023.0100)

  Note: Valid 14.2 MP1 version 14.2.1015.0100 was available for a short while with the same component versions. 14.2.1023.0100 replaces it.

Symantec AntiVirus for Linux 1.0.14 is the only version that you can migrate directly to Symantec Endpoint Protection. You must first uninstall all other versions of Symantec AntiVirus for Linux. You cannot migrate a managed client to an unmanaged client.

Unsupported upgrade paths

You cannot migrate to Symantec Endpoint Protection from all Symantec products. You must uninstall the following products before you install the Symantec Endpoint Protection client:

- The unsupported Symantec products Symantec AntiVirus and Symantec Client Security
- All Symantec Norton™ products
- Symantec Endpoint Protection for Windows XP Embedded 5.1
- Versions of Symantec Endpoint Protection for Mac earlier than 12.1.4

You cannot upgrade Symantec Endpoint Protection Manager 11.0.x or Symantec Endpoint Protection Manager Small Business Edition 12.0.x directly any version of Symantec Endpoint Protection Manager 14. You must first uninstall these versions or perform an upgrade to 12.1.x before an upgrade to 14.x.

Downgrade paths are not supported. For example, if you want to migrate from Symantec Endpoint Protection 14.2.1 to 12.1.6 MP10, you must first uninstall Symantec Endpoint Protection 14.2.1.

Increasing Symantec Endpoint Protection Manager available disk space before an upgrade

The Symantec Endpoint Protection Manager installation requires a minimum amount of available disk space. Make sure that any current 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.

Make a backup of the database before making configuration changes.

See “Backing up the database and logs” on page 754.

Table 7-3 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 **Local Site**. Select **Edit Site Properties.** 2 On the **LiveUpdate** tab, uncheck **Store client packages unzipped to provide better network performance for upgrades**. **Note:** This option was removed in version 12.1.5 because content storage on the management server is improved. You should still set it appropriately for an upgrade from a version earlier than 12.1.5, however. 3 On the **LiveUpdate** tab, reduce the number of content revisions to keep. For an upgrade, you can lower the setting to 10. Allow time for Symantec Endpoint Protection Manager to purge the extra revisions. However, for versions later than 12.1.5, the reduction of revision numbers may trigger full update downloads from the clients that check in. An increase in these full update requests may negatively affect network performance. **Note:** The default values and recommended values for content storage have also changed as of version 12.1.5. To upgrade, however, you need to work with the values that are appropriate for the version from which you upgrade. Returning the revision setting to its previous value after the upgrade completes is not necessary. Improvements to the way Symantec Endpoint Protection Manager stores and manages content means that a larger number of revisions takes up less disk space than in earlier versions. See "How to update content and definitions on the clients" on page 178. See "Downloading content from LiveUpdate to the Symantec Endpoint Protection Manager" on page 186.
Make sure that unused virus definitions are deleted from the Symantec Endpoint Protection Manager database	1 Go to **Admin > Servers**, right-click the database server, and then select **Edit Database Properties**. For the embedded database, right-click **localhost**. For a Microsoft SQL Server database, the database server name varies based on the location of your database. 2 On the **Log Settings** tab, under **Risk Log Settings**, make sure that **Delete unused virus definitions** is checked.

Table 7-3 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 Symantec Endpoint Protection Manager, consider relocating them to another server. You can remove unused programs. ■ If storage-intensive programs are installed on the same computer with Symantec Endpoint Protection Manager, consider dedicating a computer to support only Symantec Endpoint Protection Manager. ■ Remove temporary Symantec Endpoint Protection Manager files. For a list of temporary files that you can remove, see the 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 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 85.

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.

Error: "Low Disk Space" on computers running Endpoint Protection

For the most current system requirements, see: Release notes, new fixes, and system requirements for all versions of Endpoint Protection

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.

Table 7-4 Upgrade tasks

Task	Description
Upgrade the management server	Review the system requirements and supported upgrade paths, upgrade the management server, and then configure it with the Management Server Configuration Wizard. As of 14, the following applies to a Symantec Endpoint Protection Manager upgrade: ■ Windows Server 2003, all desktop operating systems, and 32-bit operating systems are no longer supported. ■ SQL Server 2005 is no longer supported for the database. Support is also dropped for SQL Server 2008 earlier than SP4, and SQL Server 2008 R2 earlier than SP3. ■ You must now enter SQL Server system administrator credentials during the upgrade. **Note:** You may need to edit the domain security policies to allow the virtual service accounts to run correctly for Windows 7 / Server 2008 R2 or later. See: Error: "...services require user rights" or "...cannot read the user rights" during installation or configuration See "Installing Symantec Endpoint Protection Manager" on page 43. See "Supported upgrade paths to the latest version of Symantec Endpoint Protection 14.x" on page 144. See "Upgrading an environment that uses multiple embedded databases and management servers" on page 151.
Log onto the management server	When the Symantec Endpoint Protection Manager logon panel appears, you can log on to the console by using your logon credentials. See "Logging on to the Symantec Endpoint Protection Manager console" on page 48.

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.

See "Setting up failover and load balancing" on page 732.

See "Setting up sites and replication" on page 739.

Upgrading an environment that uses multiple embedded databases and management servers

Upgrading an environment that uses multiple embedded database and management servers has the following implications:

- The management servers do not use failover or load balancing for Symantec Endpoint Protection because the embedded database does not support failover or load balanced servers.
- The management servers are Symantec Endpoint Protection replication partners.

All sites have a computer on which you first installed the management server. You must upgrade this management server first, because it contains critical site information such as the encryption key or encryption password. You then upgrade the other management servers that you installed for replication.

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

1. Authenticate to and log on to the computer on which you installed the first Symantec Endpoint Protection Manager.

   Do not log on to Symantec Endpoint Protection Manager. If you use replication, you do not need to disable it first. Symantec Endpoint Protection does not allow replication if the product versions do not match.

2. Upgrade the management server.

   See "Upgrading a management server" on page 149.

3. Upgrade all additional management servers one by one.

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, the 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 this 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" on page 141.

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 this procedure again, but 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
```

Disabling replication and restoring replication before and after an upgrade

Before you upgrade the management server, you should temporarily disconnect the partnership with all management servers that are configured as replication partners. If a replication partner launches replication during the upgrade, it may have unpredictable results.

Warning: Disabling replication is not the same as permanently deleting the replication partnership. If you delete the relationship and then reinstall the management server, the management servers perform a full replication instead of an incremental replication. See "Deleting sites" on page 751.

Disabling replication

You must log on to Symantec Endpoint Protection Manager and disable replication at a minimum of two sites.

To disable replication

1. In the console, click **Admin > Servers**.
2. Under **Local Site** > **Servers**, expand **Replication Partners** and select the management server.
3. Right-click the management server, and then click **Delete Replication Partner**.
4. Click **Yes**.
5. Repeat this procedure at all sites that replicate data.

Restoring a replication partner when a site has already been replicated

After you upgrade all management servers that had a replication relationship, you add the replication partner back. You must also re-add the management servers that were configured for failover and load balancing.

You only re-add replication partners on the computer on which you first upgraded the management server. The upgraded management server must also have previously been a replication partner in the same site farm.

After you add the replication partner back, Symantec Endpoint Protection Manager makes the databases consistent. However, some changes may collide.

See "How to resolve data conflicts between sites during replication" on page 743.

If you have two separate, non-replicating sites, you can also use this option to convert one of the sites into a site which replicates with the other site.

To restore replication after an upgrade

1. On the console, click **Admin > Servers**.
2. Under **Servers**, expand **Local Site**, and under **Tasks**, click **Add Existing Replication Partner**.
3. In the welcome panel, click **Next**.
4. In the **Remote Site Information** panel, type the IP address or host name for the second management server, the system administrator's logon information, and then click **Next**.

   The system administrator's user name is `admin` by default.
5. Set the replication schedule and click **Next**.
6. Check which items to replicate, and then click **Next**.

   Client package replication uses large amounts of traffic and hard disk space.

   If you click **Yes**, the management server performs a full replication of data between the two replication partners.
7. When a message appears asking whether or not you have restored the database on the partner site, click one of the following options:
   - Click **No** to replicate only the data that changed since this partner relationship was disabled. Symantec recommends this option, especially if your network has low bandwidth.
   - Click **Yes** to perform a full replication of data between the two replication partners.
8. Click **Finish**.
9. Repeat this procedure for all computers that replicate data with this computer.

See "How to install a second site for replication" on page 748.

Upgrade best practices for Endpoint Protection 14

See "Upgrading to a new release" on page 141.

Choosing which method to upgrade the client software

You can upgrade the client using multiple ways. The method you should use depends on your environment and goals. For example, you might have a large number of clients or groups, or computers that run different versions of the client.

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 7-5 Methods to upgrade the client software

Method	When to use	When not to use
AutoUpgrade (Recommended for smaller environments)	■ When you have a smaller number of clients, such as 5,000 clients or fewer. ■ When you need to schedule the upgrade to occur when the upgrade does not interrupt the users' work. ■ When you use Symantec Endpoint Protection Manager and not a third-party application to deploy the client installation package. ■ When you need to upgrade either Windows or Mac clients, but not Linux clients. ■ When you want a simple upgrade method. See "Upgrading client software with AutoUpgrade" on page 156.	■ When you have a larger number of clients. This method does not scale well. ■ When you have a lot of groups, because it is time-consuming to click each group individually in the wizard. ■ When you have a complicated upgrade schedule where you need a lot of granularity. ■ When you need to upgrade Linux clients. How to deploy the Symantec Endpoint Protection Linux client as part of a cloned drive image
Export a client installation package (Recommended for larger environments)	■ When you deploy the client installation package manually instead of with Symantec Endpoint Protection Manager. ■ When you deploy the client installation package with an existing third-party deployment application instead of with Symantec Endpoint Protection Manager. To use this method, you should have this infrastructure already in place. ■ When you need to upgrade Windows clients, Mac clients, and Linux clients. See "Exporting client installation packages" on page 136. See "Installing Windows client software using third-party tools" on page 812.	■ When you normally use Symantec Endpoint Protection Manager to update the clients.
Client Deployment Wizard	■ When you have a smaller number of clients, such as fewer than 250 clients. ■ When you deploy the client using Symantec Endpoint Protection Manager and not a third-party application. ■ When you want a simpler upgrade method. Use the **New Package Deployment**. See "Installing Symantec Endpoint Protection clients with Remote Push" on page 60.	■ When you have a large network environment, as this method does not scale well.

Table 7-5 Methods to upgrade the client software *(continued)*

Method	When to use	When not to use
Download client installation files from MySymantec	■ When you want to upgrade a few clients at a time in a few specific cases. For example: ■ If an issue occurs on a few computers with an older version of the client, and the newer version fixes the issue. ■ If you have a smaller number of clients to upgrade and do not want to upgrade the management server. ■ When you need to upgrade Windows, Mac, and Linux clients. ■ When you must deploy the client directly on the computer or by using a third-party deployment application instead of Symantec Endpoint Protection Manager. You download the standalone **All Clients** installation file from MySymantec. Getting Started with MySymantec See "Installing an unmanaged Windows client" on page 131.	If you upgrade the client on computers with existing managed clients, the clients stay managed. However, if you deploy to new computers without an existing client, this method installs an unmanaged client only. You must convert the client to a managed client later to connect to the management server. See "How do I replace the client-server communications file on the client computer?" on page 171. See "Exporting the client-server communications file (Sylink.xml) manually" on page 174.

See "Upgrading to a new release" on page 141.

Upgrading client software with AutoUpgrade

AutoUpgrade lets you automatically upgrade the Symantec Endpoint Protection client software on all of the Windows or Mac clients in a group.

With AutoUpgrade, Windows standard clients receive a delta upgrade package that Symantec Endpoint Protection Manager creates. This package is smaller than the full installation package. Windows embedded or VDI clients always receive the full installation package. These clients do not maintain a copy of the installer in the installer cache. Mac clients always receive the full installation package.

Use the following best practices for using AutoUpgrade:

- 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.

- To reduce bandwidth during peak hours, schedule AutoUpgrade for after hours in the **Upgrade Clients with Package** wizard, especially for client groups with reduced-size clients. For wide area networks, you should also set up the remote clients to receive the upgrade package from a remote web server.
- Since AutoUpgrade was first included in the Mac client with Symantec Endpoint Protection 14, you cannot upgrade with AutoUpgrade from a version earlier than 14.
- After you upgrade Symantec Endpoint Protection Manager, run LiveUpdate in the console at least once before you use AutoUpgrade to upgrade the clients.
  See "Checking that Symantec Endpoint Protection Manager has the latest content" on page 190.
- AutoUpgrade can only install the Application Hardening feature on client computers when the following conditions are met:
  - You must enable **Maintain existing client features when updating** when you run **Upgrade Clients with Package**. This setting is enabled by default.
  - The client computer cannot have the Symantec Data Center Security agent installed.
  - The Virus and Spyware Protection feature is currently installed and selected for upgrade.

See "Choosing which method to upgrade the client software" on page 154.

To upgrade client software with AutoUpgrade

1. In the console, click **Admin** > **Install Packages**.
2. Under **Tasks**, click **Upgrade Clients with Package**.
3. In the **Upgrade Clients Wizard** panel, click **Next**, select the appropriate client installation package, and then click **Next**.
4. Select the group or groups that contain the client computers that you want to upgrade, and then click **Next**.
5. Select from where the client should download the package from the following options:
   - To download from the Symantec Endpoint Protection Manager server, click **Download from the management server**.
   - To download from a web server that is local to the computers that need to update, click **Download from the following URL (http or https)**. Enter the URL of the client installation package into the provided field.
6. Click **Upgrade Settings** to specify upgrade options.
7. On the **General** tab, under **Client Settings**, choose from the following options, depending on the client operating system:
   - For Windows, use the drop-down menus to select options for **Maintain existing client features when updating** and **Install Settings**.

Note: If you deselect **Maintain existing client features when updating**, you can optionally add or remove features when upgrading.

- For Mac, use the drop-down menu to select options for **Install Settings**.
- For Windows, **Content Selection** lets you include content in the installation package. If you include content, the package is larger, but the client has up-to-date content immediately after installation. If you do not include content, the package is smaller, but the client must get content updates after installation.

You can also add an optional upgrade schedule. Without a schedule, the AutoUpgrade process begins after the wizard completes.

8 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.

9 Click **OK**, and then click **Next**.

10 In the **Upgrade Clients Wizard Complete** panel, click **Finish**.

To confirm the version number of the client software

- After the upgrade completes, you can check the version to confirm a successful upgrade in one of the following ways:
  - In the console, click **Clients > Clients**, select the appropriate group, and change the view to **Client Status**.
  - On the Windows client, in the Symantec Endpoint Protection client interface, click **Help** > **About**.
  - On the Mac client, open the Symantec Endpoint Protection client interface. In the menu bar, click **Symantec Endpoint Protection > About Symantec Endpoint Protection**.

The client computer must restart after the upgrade. By default, the clients restart after installation. You can configure the restart options in the group's general settings to control how the clients in a group restart after AutoUpgrade. You can also restart the clients at any time by running a restart command from the management server.

See "Restarting the client computers from Symantec Endpoint Protection Manager" on page 127.

See "Applying upgrade settings to other groups" on page 158.

Applying upgrade settings to other groups

You can copy existing AutoUpgrade client installation package upgrade settings from one group to another group. If you copy upgrade settings, you don't have to create the package settings for each group individually.

This option copies the following client install package settings:

- The client feature set
- Whether **Maintain existing client features when updating** is enabled or disabled
- The client installation settings
- The content selection
- The download source
- The upgrade schedule
- The settings and message text from the **Notifications** tab

The Windows settings apply to Windows clients and the Mac settings apply to Mac clients during AutoUpgrade. They also apply to any new client that joins the group.

If you apply the copied settings to a package that is already assigned to a target group, the copied settings override the target group's existing settings. If the target group has no assigned package, this option adds a client install package with the copied settings.

To apply upgrade settings to other groups

1. In the console, do one of the following tasks:
   - Click **Clients** > **Install Packages**, select the group, and under **Tasks**, click **Apply current deployment settings to other groups**.
   - Click **Clients**, right-click a group, and then click **Copy Deployment Settings**.
2. In the **Copy Deployment Settings** dialog box, click the new groups, click **OK**, and then click **Yes**.

See "Upgrading client software with AutoUpgrade" on page 156.

Upgrading Group Update Providers

Use this procedure to upgrade the clients that are Group Update Providers.

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.

See "Using Group Update Providers to distribute content to clients" on page 215.

See "Upgrading to a new release" on page 141.

Section 2

Managing client-server communication and updating content

Chapter 8

Managing client-server communication

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.

Table 8-1 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 "Checking whether the client is connected to the management server and is protected" on page 163. A computer may have the client software installed, but does not have the correct communications file. See "How does the client computer and the management server communicate?" on page 168. See "How do I replace the client-server communications file on the client computer?" on page 171.
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 168. See "Updating client policies" on page 313.
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 "Updating policies and content on the client using push mode or pull mode" on page 165.
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 for load balancing" on page 736.
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 272.
Troubleshoot management server connectivity problems	If the management server and the client do not connect, you can troubleshoot connection problems. See "Troubleshooting connectivity problems between Symantec Endpoint Protection Manager and the Symantec Endpoint Protection client" on page 765.

For more information, see the following article: About the communication ports that Symantec Endpoint Protection uses

Checking whether the client is connected to the management server and is protected

After you install the client, check whether the clients are online and connected to the Symantec Endpoint Protection Manager. You can check the connection status on both the console and on the client.

To check the client-management server connection on the Symantec Endpoint Protection client

- On the client computer, do one of the following tasks:
  - The client shield in the computer's taskbar has a green dot.

    
  - Open the client and look on the Status screen, which states that **Your computer is protected** and displays a green check mark.

    
  - Open the client and click **Help** > **Troubleshooting**.

See "Symantec Endpoint Protection client status icons" on page 165.

To check the client-management server connection in Symantec Endpoint Protection Manager

1. In the console, click **Clients** and select the target group.
2. On the **Clients** tab, clients that are connected display an icon with a green dot in the **Name** column and display a health state of **Online**.

Note: Clients that connect through Symantec Endpoint Protection Manager may not immediately display the correct online status in the cloud console. Allow for 5-10 minutes after the online status changes to see an accurate reflection of the current status.

Version 14	Version 12.1.x
	

Table 8-2 displays what the following icons in the **Name** column mean.

Table 8-2 Client status icons in the management console

14	12.1.x	Description
		The client software installation failed.
		■ The client can communicate with Symantec Endpoint Protection Manager. The health state is **Online**. ■ The client is in computer mode.
		■ The client cannot communicate with Symantec Endpoint Protection Manager. The health state is **Offline**. ■ The client is in computer mode. ■ The client may have been added from the console, and may not have any Symantec client software installed.
		■ The client can communicate with Symantec Endpoint Protection Manager. ■ The client is in computer mode. ■ The client is an unmanaged detector.
		■ The client cannot communicate with Symantec Endpoint Protection Manager. ■ The client is in computer mode. ■ The client is an unmanaged detector.
		■ The client can communicate with Symantec Endpoint Protection Manager. ■ The client is in user mode.
		■ 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.
		■ The client can communicate with Symantec Endpoint Protection Manager at another site. ■ The client is in computer mode.
		■ The client can communicate with Symantec Endpoint Protection Manager at another site. ■ The client is in computer mode. ■ The client is an unmanaged detector.
		■ The client can communicate with Symantec Endpoint Protection Manager at another site. ■ The client is in user mode.

See "Viewing the protection status of client computers" on page 247.

Symantec Endpoint Protection client status icons

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 notification area icon is sometimes referred to as the system tray icon.

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 8-3 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 client runs with no problems. It is connected to and communicates with the server. All components of the security policy protect the computer.
	The client has a minor problem. For example, the virus definitions may be out of date.
	The client does not run, has a major problem, has an expired license, or has at least one protection technology disabled.

You can also check the management server to view the connection status of the computers.

See “Checking whether the client is connected to the management server and is protected” on page 163.

See “Running a report on the deployment status of clients” on page 631.

See “Managing the client-server connection” on page 161.

Updating policies and content on the client using push mode or pull mode

Deciding whether to use pull mode or push mode to connect between Symantec Endpoint Protection Manager and the clients

Configuring push mode or pull mode for a group

Deciding whether to use pull mode or push mode to connect between Symantec Endpoint Protection Manager and the clients

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.

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. 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 168.

See "Communication ports for Symantec Endpoint Protection" on page 112.

Configuring push mode or pull mode for a group

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 "Performing the tasks that are common to all policies" on page 313.

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

To configure push mode or pull mode for a group

1. In the console, click **Clients**.
2. 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 313.

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 "Updating client policies" on page 313.

See "Updating policies and content on the client using push mode or pull mode" on page 165.

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 313.

How does the client computer and the management server communicate?

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.

The sylink file performs many of its functions during the heartbeat. The heartbeat is the frequency at which client computers upload logs to the management server, and download policies and commands.

The sylink file contains:

- The public certificate for all management servers.
- The KCS, or encryption key.
- The Domain ID that each client belongs to.

Note: Do not edit the sylink file. If you change the settings, the management server overwrites most settings the next time the client connects to the management server.

See "Updating policies and content on the client using push mode or pull mode" on page 165.

Troubleshooting Sylink communication

In version 14.2, the communications module was upgraded, and includes new log files. You can use this information to troubleshoot communication issues between Symantec Endpoint Protection Manager and the clients.

The 14.2 communications module works with all client types, including Windows, Mac, and Linux, and has improved IPv6 support.

Note: As of version 14.2, the communication module only honors system proxy information.

To view the log files for the communications module

- On the Windows client, in the following folder:

  `C:\ProgramData\Symantec\Symantec Endpoint Protection\CurrentVersion\Data`

  You can view the following files:

  - **For client registration:**
    - `RegistrationInfo.xml`
      Client registration metadata that the client submits to Symantec Endpoint Protection Manager.
    - `Registration.xml`
      Client registration metadata that Symantec Endpoint Protection Manager returns to the client.
    - `State.xml`
      Includes internal settings, such as the management server IP address.

- **For the communications module logs:**
  `\Logs\cve.log` and `\Logs\cve-actions.log`
  Use these logs to troubleshoot communication between Symantec Endpoint Protection Manager and the client. Send these logs to Technical Support if asked.
- **For the opstate status:**
  Appears in the logs in the `\Pending` and `\Sent` folders

To configure the communication module logs

1 Open the Windows Registry Editor, click **Start** > **Run**, type `regedit`, and then click **OK**.

2 To enable the cve.log or cve-actions.log, open the following Windows registry key:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint
Protection\SMC\SYLINK\SyLink REG_DWORD: CVELogLevel
```

Use any of the following values:

- 1 = Debug
- 2 = Info
- 3 = Warning
- 4 = Error
- 5 = Fatal

If the registry key is not present or does not have a valid value, it defaults to 4. The installation default is also 4.

For example, you can type:

32-bit: `[HKLM\SOFTWARE\Symantec\Symantec Endpoint Protection\SMC\SYLINK\SyLink] "CVELogLevel"=dword:00000001`

64-bit: `[HKLM\SOFTWARE\Wow6432Node\Symantec\Symantec Endpoint Protection\SMC\SYLINK\SyLink] "CVELogLevel"=dword:00000001`

3 To control the size of these logs, use the following registry value:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\SOFTWARE\Symantec\Symantec Endpoint
Protection\SMC\SYLINK\SyLink] REG_DWORD: CVELogSizeDB
```

The default size is 250 MB.

How to enable Communication Module logging in Endpoint Protection 14.2

How do I replace the client-server communications file on the client computer?

When should I replace the client-server communications file on the client computer?

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 "Checking the connection to the management server on the client computer" on page 767.
- You want to convert an unmanaged client to a managed client. If a user installs a client from the installation file, 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 129.
- 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 on the orphaned clients to re-establish communication with them.
  See "Update the server certificate on the management server without breaking communications with the client" on page 709.
  See "Exporting the client-server communications file (Sylink.xml) manually" on page 174.
- 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 243.

How do I replace the client-server communications file on the client computer?

See "Restoring client-server communications with Communication Update Package Deployment" on page 173.

How to convert an unmanaged Symantec Endpoint Protection for Macintosh client to managed

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 with Communication Update Package Deployment" on page 173.
- Write a script that runs the SylinkDrop tool, which is located in the \Tools folder of the installation file. 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 772.
- 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. 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 8-4 displays the process for exporting and importing the Sylink.xml file into the client computer.

Table 8-4 Steps for exporting and importing the communications file

Step	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 (Sylink.xml) manually" on page 174.
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.
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 Windows client" on page 175. 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 Symantec Endpoint Protection client" on page 260. You do not need to restart the client computer.

Table 8-4 Steps for exporting and importing the communications file *(continued)*

Step	Description
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 "Checking whether the client is connected to the management server and is protected" on page 163.

See "Client and server communication files" on page 776.

See "How does the client computer and the management server communicate?" on page 168.

Restoring client-server communications with Communication Update Package Deployment

If the client-server communications break, you can quickly restore communications by replacing the Sylink.xml file on the client computer. You can replace the Sylink.xml file by deploying a communication update 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 "How does the client computer and the management server communicate?" on page 168.

To restore client-server communication settings with Communication Update Package Deployment

1. In the console, launch the **Client Deployment Wizard**.

   Click **Help > Getting Started Page** and then under **Required tasks**, click **Install the client software on your computers**.

2. In the **Client Deployment Wizard**, under **Communication Update Package Deployment**, select whether you want a package for Windows or Mac clients, and then click **Next**.

3. Select the group on which you want to apply the policy, and then click **Next**.

   For Windows clients only, you can set password protection.

   See "Password-protecting the Symantec Endpoint Protection client" on page 260.

4. Choose one of the following deployment methods, and then click **Next**:

   - Click **Remote Push** and go to the **Computer Selection** step in the following procedure.
     See "Installing Symantec Endpoint Protection clients with Remote Push" on page 60.

- **Save Package** and go to the **Browse** step in the following procedure.
  See "Installing Symantec Endpoint Protection clients with Save Package" on page 53.

5 After the communication update package is applied, confirm that the computers successfully communicate with Symantec Endpoint Protection Manager.

  See "Checking whether the client is connected to the management server and is protected" on page 163.

  See "Running a report on the deployment status of clients" on page 631.

Exporting the client-server communications file (Sylink.xml) manually

If the client and the server do not communicate, you may need to replace 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 on the client are:

- To convert an unmanaged client into a managed client.
- To reconnect a previously orphaned client to the management server.
  See "Update the server certificate on the management server without breaking communications with the client" on page 709.

See "How does the client computer and the management server communicate?" on page 168.

If you need to update client-server communications for a large number of clients, deploy the Communication Update Package instead of using this method.

See "Restoring client-server communications with Communication Update Package Deployment" on page 173.

To export the client-server communications file manually

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

2 Under **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 Under **Preferred Policy Mode**, make sure that **Computer Mode** is checked.

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 Windows client" on page 175.

Importing client-server communication settings into the Windows client

Once you have exported client-server communication settings, you can import them into a Windows client. You can use it to convert an unmanaged client into a managed client or to reconnect a previously orphaned client with Symantec Endpoint Protection Manager.

To import the client-server communications settings file into the Windows 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 appears with a green dot 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 (Sylink.xml) manually" on page 174.

See "Restoring client-server communications with Communication Update Package Deployment" on page 173.

Importing client-server communication settings into the Linux client

After you install an unmanaged Symantec Endpoint Protection for Linux client, you can convert it to a managed client to centrally manage the client's policies and status with Symantec

Endpoint Protection Manager. A managed client communicates with and reports its status and other information to Symantec Endpoint Protection Manager.

You can also use this procedure to reconnect a previously orphaned client with Symantec Endpoint Protection Manager.

Note: You must have superuser privileges to perform this procedure. The procedure uses `sudo` to demonstrate this elevation of privilege as required.

The text *path-to-sav* represents the path to the sav command. The default path is /opt/Symantec/symantec_antivirus/.

To import the client-server communication settings file into the Linux client

1. You or the Symantec Endpoint Protection Manager administrator must first export the communication settings file from Symantec Endpoint Protection Manager and copy it to the Linux computer. Ensure that the file name is `sylink.xml`.

   See "Exporting the client-server communications file (Sylink.xml) manually" on page 174.

2. On the Linux computer, open a terminal window and enter the following command:

   `sudo` *`path-to-sav`*`/sav manage -i` *`path-to-sylink`*`/sylink.xml`

   Where *path-to-sylink* represents the path to which you copied `sylink.xml`.

   For example, if you copied it to your user profile's desktop, enter:

   `sudo` *`path-to-sav`*`/sav manage -i ~/Desktop/sylink.xml`

3. A successful import returns OK. To further verify the managed status, enter the following command, which displays the policy serial number for a successful import:

   `path-to-sav``/sav manage -p`

See "Installing the Symantec Endpoint Protection client for Linux" on page 58.

Chapter 9

Updating content on the clients

This chapter includes the following topics:

- Using Group Update Providers to distribute content to clients
- Using Intelligent Updater files to update content on Symantec Endpoint Protection clients
- Using third-party distribution tools to update client computers
- Downloading Endpoint Protection security patches to Windows clients

How to update content and definitions on the clients

By default, the Symantec Endpoint Protection Manager downloads content updates from the public Symantec LiveUpdate servers. Symantec Endpoint Protection clients then download these updates from the Symantec Endpoint Protection Manager. The content includes virus definitions, intrusion prevention signatures, and Host Integrity templates, among others.

Table 9-1 Steps to update content on the Symantec Endpoint Protection clients

Task	Description
Make sure that the management server has the latest content from LiveUpdate (Recommended)	By default, LiveUpdate runs as part of the Symantec Endpoint Protection Manager installation. You may need to run LiveUpdate manually in the following situations: ■ You skipped LiveUpdate during installation. ■ You must run LiveUpdate to download the Host Integrity templates and intrusion prevention signatures. ■ You want to run LiveUpdate before the next scheduled update. See "Checking that Symantec Endpoint Protection Manager has the latest content" on page 190. You can also update content on Symantec Endpoint Protection Manager with a .jdb file. Download .jdb files to update definitions for Endpoint Protection Manager Additionally, if you use replication, you can replicate content and policies between the local site and the partner site. See "How to install a second site for replication" on page 748.
Change how client computers get updates (Optional)	By default, Windows client computers get content updates from the management server. Other delivery methods include Group Update Providers, internal LiveUpdate servers, or third-party tool distribution. You may need to change the delivery method to support different client platforms, large numbers of clients, or network limitations. See "Choose a distribution method to update content on clients" on page 179. See "Choose a distribution method to update content on clients based on the platform" on page 184.

Table 9-1 Steps to update content on the Symantec Endpoint Protection clients *(continued)*

Task	Description
Change the LiveUpdate settings for the management server (Optional)	You can customize the frequency of LiveUpdate sessions, the protection components that are downloaded, and more. See "Downloading content from LiveUpdate to the Symantec Endpoint Protection Manager" on page 186.
Reduce network overloads (Recommended)	If the management server receives too many concurrent requests for full definition packages from the clients, the network may become overloaded. You can mitigate the risk of these overloads, and stop clients from downloading full definitions. See "Mitigating network overloads for client update requests" on page 205.
Improve performance (Recommended)	To help mitigate the effect of downloads on network bandwidth, download content randomly so that not all clients get updates at the same time. See "About randomization of simultaneous content downloads" on page 205. See "Randomizing content downloads from the default management server or a Group Update Provider" on page 206. See "Randomizing content downloads from a LiveUpdate server" on page 207. 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 Windows client updates to run when client computers are idle" on page 208.
Let your endpoint users manage their own updates (Optional)	By default, users on the client computer can run LiveUpdate at any time. 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 204. You can also use an Intelligent Updater file on a client computer to update the definitions. See "Using Intelligent Updater files to update content on Symantec Endpoint Protection clients" on page 223.
Test engine updates before Symantec releases them (Optional)	Symantec releases engine updates on a quarterly basis. You can download the engine updates before they are released using a specific Symantec LiveUpdate server. You can then test the engine content before you roll out the content to your production environment. See "Testing engine updates before they release on Windows clients" on page 210.

Choose a distribution method to update content on clients

You may need to change the default update method to the clients, depending on the client platform, network configuration, number of clients, or your company's security policies and access policies.

Table 9-2 Content distribution methods and when to use them

Method	Description	When to use it
Symantec Endpoint Protection Manager to client computers (default) (Windows, Mac, Linux)	The default management server automatically updates the client computers that it manages. You do not define the schedule for the updates from the management server to the clients. The clients download content from the management server based on the communication mode and heartbeat frequency. See "Configuring clients to download content from the Symantec Endpoint Protection Manager" on page 210. See "Updating policies and content on the client using push mode or pull mode" on page 165.	Symantec recommends that you use this method unless network constraints or your company's policies require an alternative. If you have a large number of clients or bandwidth issues, you might use this method, along with Group Update Providers. For Mac or Linux computers to receive content updates from the management server, you must configure the Apache web server. Enabling Mac and Linux clients to download LiveUpdate content using the Apache Web server as a reverse proxy
Group Update Provider to client computers (Windows only)	A Group Update Provider is a client computer that receives updates from a management server. The Group Update Provider then forwards the updates to the other client computers in the group. A Group Update Provider can update multiple groups. Group Update Providers can distribute all types of LiveUpdate content except client software updates. Group Update Providers also cannot be used to update policies.	A Group Update Provider lets you reduce the load on the management server, and is easier to configure than an internal LiveUpdate server. Use a Group Update Provider for groups at remote locations with minimal bandwidth. See "Using Group Update Providers to distribute content to clients" on page 215. See "Deciding whether or not to set up multiple sites and replication" on page 744.

Table 9-2 Content distribution methods and when to use them *(continued)*

Method	Description	When to use it
Internal LiveUpdate server to client computers (Windows, Mac, Linux)	Client computers can download updates directly from an internal LiveUpdate server that receives its updates from a Symantec LiveUpdate server. If necessary, you can set up several internal LiveUpdate servers and distribute the list to client computers. You can change the download schedule from the LiveUpdate server to the management server. See "Configuring the LiveUpdate download schedule to client computers" on page 202. For more information about setting up an internal LiveUpdate server, see the *LiveUpdate Administrator User's Guide* at: Downloading LiveUpdate Administrator	An internal LiveUpdate server lets you reduce the load on the management server in very large networks. In smaller networks, consider whether Group Update Providers would meet your organization's needs. Consider using an internal LiveUpdate server in the following situations: ■ If you manage a large network (more than 10,000 clients) ■ If you manage Mac or Linux clients that should not connect to an external LiveUpdate server ■ If your organization deploys multiple Symantec products that also use LiveUpdate to distribute content to client computers **Note:** You should not install the management server 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: LiveUpdate Administrator 2.x and Symantec Endpoint Protection Manager on the same computer See "Configuring clients to download content from an internal LiveUpdate server" on page 196.

Table 9-2 Content distribution methods and when to use them *(continued)*

Method	Description	When to use it
External Symantec LiveUpdate server to client computers over the Internet (Windows, Mac, Linux)	Client computers can receive updates directly from a Symantec LiveUpdate server.	Use an external Symantec LiveUpdate server if you need to schedule when clients update content or if the available bandwidth between the Symantec Endpoint Protection Manager and the clients is limited. Symantec Endpoint Protection Manager and scheduled updates are enabled by default. With the default settings, clients always get updates from the management server unless management server is unresponsive 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 bandwidth. See "Configuring clients to download content from an external LiveUpdate server" on page 200.
Third-party tool distribution (Windows only)	Third-party tools like Microsoft SMS let you distribute specific update files to clients.	This method lets you test update files before you distribute them. It may also make sense if you have a third-party tool distribution infrastructure in place. See "Distributing the content using third-party distribution tools" on page 227.
Intelligent Updater (Windows only)	Intelligent Updater files contain the virus and security risk content and intrusion prevention 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 LiveUpdate is not available. See "Using Intelligent Updater files to update content on Symantec Endpoint Protection clients" on page 223. 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 225.

Figure 9-1 shows an example distribution architecture for smaller networks.

Figure 9-1 Example distribution architecture for smaller networks

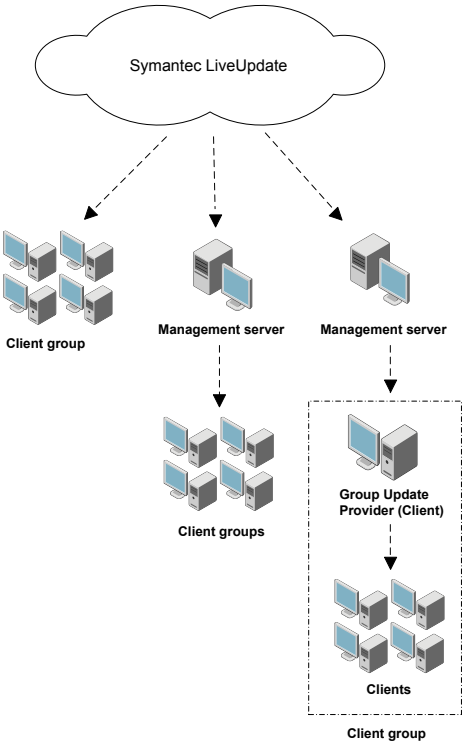
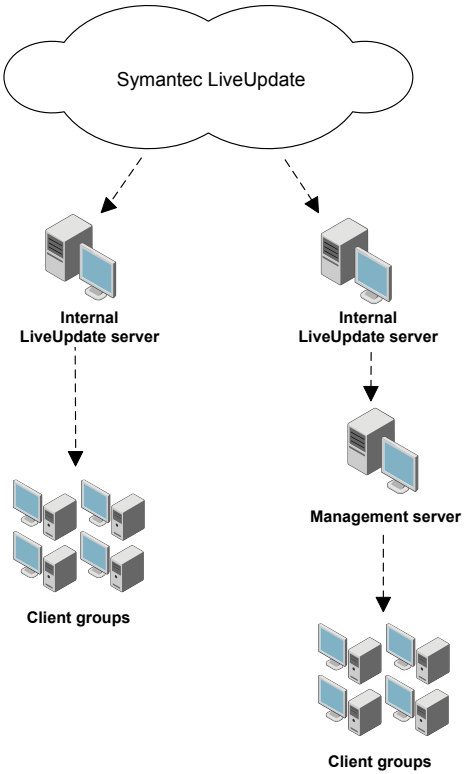


Figure 9-2 shows an example distribution architecture for larger networks.

Figure 9-2 Example distribution architecture for larger networks



See "Choose a distribution method to update content on clients based on the platform" on page 184.

See "How to update content and definitions on the clients" on page 178.

See "Downloading content from LiveUpdate to the Symantec Endpoint Protection Manager" on page 186.

Choose a distribution method to update content on clients based on the platform

The methods that you can use to distribute virus definitions and other content to the client computers depends on the client platform.

Table 9-3 Content distribution method based on Windows, Mac, and Linux clients

Platform	Method
Windows	By default, the Windows client gets content from the management server. Windows clients can also get updates from the following sources: ■ A LiveUpdate server (external or internal) See "Configuring clients to download content from an internal LiveUpdate server" on page 196. See "Configuring clients to download content from an external LiveUpdate server" on page 200. ■ An external LiveUpdate server (testing only) See "Testing engine updates before they release on Windows clients" on page 210. ■ A Group Update Provider See "Using Group Update Providers to distribute content to clients" on page 215. ■ Third-party distribution tools See "Distributing the content using third-party distribution tools" on page 227. ■ Intelligent Updater See "Using Intelligent Updater files to update content on Symantec Endpoint Protection clients" on page 223. See "Choose a distribution method to update content on clients" on page 179. For Windows clients, you can also customize the following settings: ■ The content types that the client receives ■ Whether the client can get definitions from multiple sources ■ Whether the client can get smaller packages (deltas) from LiveUpdate if the management server can provide only full definition packages Full definition packages are very large. Too many downloads of full packages can overload your network. Deltas are typically much smaller, and affect your network bandwidth much less. See "Mitigating network overloads for client update requests" on page 205.
Mac or Linux	■ A LiveUpdate server (external or internal) ■ An Apache Web server that you configure as a reverse proxy Enabling Mac or Linux clients to download LiveUpdate content using the Apache Web server as a reverse proxy

See "Downloading content from LiveUpdate to the Symantec Endpoint Protection Manager" on page 186.

See "About the types of content that LiveUpdate downloads" on page 191.

See "How to update content and definitions on the clients" on page 178.

Downloading content from LiveUpdate to the Symantec Endpoint Protection Manager

When you configure the management server to download LiveUpdate content, you have to make a number of decisions. When you download content to Symantec Endpoint Protection Manager, you download the content for all the management servers in the site.

Decisions to make about downloading content

Table 9-4 Decisions about content downloads

Decision	Description
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. 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:** Symantec Endpoint Protection Manager no longer includes legacy support for LiveUpdate Administrator 1.x. To continue using an internal LiveUpdate server, you should upgrade to the latest version of LiveUpdate Administrator. Downloading LiveUpdate Administrator See "Configuring clients to download content from an external LiveUpdate server" on page 200. See "Configuring clients to download content from an internal LiveUpdate server" on page 196. See "Choose a distribution method to update content on clients" on page 179.

Table 9-4 Decisions about content downloads *(continued)*

Decision	Description
How many content revisions should the site store?	LiveUpdate content revisions are stored differently on the management server than in Symantec Endpoint Protection Manager versions earlier than 12.1.5. Earlier releases stored full content for every revision. Now, the server stores only the most recent full content package, plus incremental deltas for as many revisions as you specify here. This approach reduces the disk space that is required to store multiple content revisions on the server. The number of clients you select during the Symantec Endpoint Protection Manager installation defines the number of revisions the server stores. For each LiveUpdate content type, the default values are as follows: For 14: ■ If you do not check **Management server will manage fewer than 500 clients**, Symantec Endpoint Protection Manager stores 21 revisions. ■ If you check **Management server will manage fewer than 500 clients**, Symantec Endpoint Protection Manager stores 90 revisions. For versions earlier than 14 but later than 12.1.5, or for upgrades from versions earlier than 14: ■ If you select fewer than 100 clients, Symantec Endpoint Protection Manager stores 12 revisions. ■ If you select 100 to 500 clients, Symantec Endpoint Protection Manager stores 21 revisions. ■ If you select 500 to 1,000 clients, Symantec Endpoint Protection Manager stores 42 revisions. ■ If you select more than 1,000 clients, then Symantec Endpoint Protection Manager stores 90 revisions. In most instances during an upgrade, the installation increases the number of revisions to match these new defaults. This increase occurs if the number of revisions you had before the upgrade is less than the new minimum default, based on the above criteria. See "Reverting to an older version of the Symantec Endpoint Protection security updates" on page 213.
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.
What operating systems am I downloading content to?	LiveUpdate only downloads the content for the specified operating systems.

Table 9-4 Decisions about content downloads *(continued)*

Decision	Description
What content types should I download to the site and to the clients?	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 downloads" on page 191. See "Reverting to an older version of the Symantec Endpoint Protection security updates" on page 213.
What languages should be downloaded for product updates?	This setting applies to product updates only; the content updates are downloaded automatically for all languages.
What content size should be downloaded for definitions?	Version 14 standard and embedded/VDI clients use a reduced-size set of definitions (only the latest) that is cloud-enabled. Scans on these clients automatically use the extended definitions set in the cloud. 14 also includes a dark network client that downloads the entire set of definitions. 12.1.x standard clients require legacy standard-size content, which includes the entire set of definitions. 12.1.6.x embedded/VDI clients require legacy reduced-size content. **Warning:** Your management server must download the correct content for the client types in your network. If the management server does not download the content that your installed clients require, the clients cannot get updates from the management server.
Should I test engine updates before they are released?	For large organizations, you should test the new engine updates and definitions before they are rolled out to all client computers. You want to test new engine updates with the minimal amount of disruption and downtime. See "Testing engine updates before they release on Windows clients" on page 210.

Downloading content from a LiveUpdate server to the Symantec Endpoint Protection Manager

When you download content to a management server, you download it for all the management servers within the site.

To configure a site to download content

1. In the console, click **Admin** > **Servers**.
2. Under **Servers**, right-click **Local Site**, and then click **Edit Site Properties**.
3. On the **LiveUpdate** tab, make choices from the following available options.

4 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 the 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**.

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.symanteclive update.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*.

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

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

6 In the **Download Schedule** group box, click **Edit Schedule**, set the options for how often the server should check for updates. Click **OK**.

7 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.

8 Under **Content Types to Download**, inspect the list of update types that are downloaded.

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.

9 Under **Content to Download for Client Types**, decide whether to download and store content for standard and embedded/VDI clients or dark network clients. You should also download and store reduced-size content or standard-size content if you run 12.1.x clients in your network.

Warning: You must download content for the client types in your network. If you do not download the content that your installed clients require, the clients cannot get updates from the management server.

To modify the setting, click **Change Selection**, modify the selection, and then click **OK**.

10 Under **Languages to Download**, inspect the list of languages of the update types that are downloaded.

To add or delete a language, click **Change Selection**, modify the list, and then click **OK**.

11 Click **OK** to save your selections and close the window.

See "How to update content and definitions on the clients" on page 178.

Checking that Symantec Endpoint Protection Manager has the latest content

LiveUpdate downloads definitions and other content to Symantec Endpoint Protection Manager on a schedule. However, you can download content at any time if Symantec Endpoint Protection Manager does not have the latest version. Symantec Endpoint Protection Manager then provides this content to the client computers through the default LiveUpdate policy.

To check that Symantec Endpoint Protection Manager has the latest content

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

2 In the Endpoint Status group box, under **Windows Definitions**, compare the dates for **Latest on Manager** and **Latest from Symantec**.

3 If the dates do not match, click **Admin** > **Servers** > **Local Site (My Site)**.

4 Under **Tasks**, click **Download LiveUpdate content** > **Download**.

If you are unable to update content on Symantec Endpoint Protection Manager through LiveUpdate, you can download a .jdb file from Symantec Security Response. Symantec Endpoint Protection Manager processes the contents of these files and makes them available for clients to download.

Download .jdb files to update definitions for Endpoint Protection Manager

Checking when content was downloaded from LiveUpdate to Symantec Endpoint Protection Manager

You can determine the date and time when content was last updated on Symantec Endpoint Protection Manager from LiveUpdate.

To check which content was downloaded from LiveUpdate to Symantec Endpoint Protection Manager

1. In the console, click **Admin**.
2. On the **Admin** page, under **Tasks**, click **Servers** and select the site.
3. Do either one of the following tasks:
   - To check the status of the download, click **Show the LiveUpdate Status**.
   - To check the version of the current content that the Symantec Endpoint Protection Manager is using, click **Show the LiveUpdate Status**.
4. Click **Close**.

Troubleshoot LiveUpdate and definition issues with Endpoint Protection Manager

See "Downloading content from LiveUpdate to the Symantec Endpoint Protection Manager" on page 186.

About the types of content that LiveUpdate downloads

By default, Symantec Endpoint Protection Manager downloads all types of content from the public Symantec LiveUpdate servers. The LiveUpdate Content policy then downloads all types of content from Symantec Endpoint Protection Manager to the Windows and Mac clients.

If you do exclude a content type from the site but you remove the content in a LiveUpdate Content policy, that content is not delivered to the clients. Typically, you should not need to exclude the content that Symantec Endpoint Protection Manager downloads. Do not exclude a type of content unless you are certain that you do not need it.

See "Reverting to an older version of the Symantec Endpoint Protection security updates" on page 213.

LiveUpdate does not download updated policies. Symantec Endpoint Protection Manager updates policies to clients when you assign a new policy to a group or when you edit an existing policy.

Table 9-5 The content types that you can download from LiveUpdate to the Symantec Endpoint Protection Manager

Content type	Description
Client product updates	Symantec recommends that you keep this setting unchecked. Product updates are improvements to the installed client software. However, while it is possible to obtain product updates by using LiveUpdate, Symantec Endpoint Protection does not usually use this method. Instead, Symantec releases a new version of the software through MySymantec. You then upgrade the management server software and the client software. You can use the **Client Deployment Wizard** to update your Mac and Linux clients using the **Web link and email** and **Save package** options. See "Upgrading to a new release" on page 141. See "Upgrading client software with AutoUpgrade" on page 156.
Client security patches	Protects against security vulnerabilities in the Windows client that have been released to the public. For example, an attacker could bypass a Symantec Endpoint Protection protection feature. The **Client Security Patches Settings** check box on a **LiveUpdate Settings** policy > **Additional Settings** tab lets you update security patches through LiveUpdate, the management server, or a Group Update Provider.
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 as well as Power Eraser definitions.
SONAR heuristic signatures	Protects against zero-day attack threats.
Intrusion Prevention signatures	Protects against network threats and host vulnerabilities. Supports the intrusion prevention and detection engines and Memory Exploit Mitigation.
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 custom requirement from a template" on page 616.
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.
Extended File Attributes and Signatures	Used to make updating certificates and Download Insight more data-driven. These data-driven downloads help Symantec update trusted signature lists with definition-style updates.

Table 9-5 The content types that you can download from LiveUpdate to the Symantec Endpoint Protection Manager *(continued)*

Content type	Description
Endpoint Detection and Response	Definitions that the Endpoint Detection and Response (EDR) component uses to detect and investigate suspicious activities and issues on hosts and endpoints. EDR provides this forensic information to various product components, including submissions and EDR servers.
Common Network Transport Library and Configuration	Definitions that the entire product uses to achieve network transportation and telemetry. These definitions are necessary for reputation queries, as well as for submissions and communication with EDR. Definitions in this category include SEPM STIC and SEPC STIC, for the Symantec Endpoint Protection Manager and Symantec Endpoint Protection client, respectively.
Advanced Machine Learning	Definitions that are used in virus and spyware scans for the clients that use a low-bandwidth policy (added in 14.0.1). Use low-bandwidth mode for standard clients and embedded clients in a network with a slow Internet connection. In low-bandwidth mode, LiveUpdate downloads the definitions once per week or less frequently. To use low-bandwidth mode, you must enroll in the cloud and enable the Low Bandwidth policy. Low-bandwidth mode does not with dark network clients. If you do not enroll the management server in the cloud console, or you do not intend on using a low-bandwidth policy, disable this option to save some bandwidth and disk space on Symantec Endpoint Protection Manager. See "Updating clients in low-bandwidth environments" on page 593.
WSS Traffic Redirection	Definitions that the Web Security Services (WSS) Traffic Redirection feature uses. WSS Traffic Redirection uses WSS servers to provide secure proxy settings for you web browsers. (Added in 14.0.1 MP1.)
Application Control content	Definitions that the Application Control engine uses for the Application Control policy. You should always keep this option enabled. This content runs on version 14.2 and later clients only. For legacy Windows clients, you must upgrade them to 14.2 first.
Policy Command Handler	Content used by the Policy Command Handler engine.
Endpoint Threat Defense for AD Data	Content used by the Active Directory Defense engine. Added for 14.2 RU1.
Symantec Endpoint Protection Manager Metadata 14.2 RU1	Data-driven information that Symantec Endpoint Protection Manager requires for the display of policy options. You should keep this content enabled except for troubleshooting purposes. Added for 14.2 RU1.

You cannot disable the following types of content in the LiveUpdate Content policy, including **Extended File Attributes and Signatures**, **Endpoint Detection and Response**, **Common Network Transport Library and Configuration**.

Table 9-6 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. ■ Centralized Reputation Settings When you configure content types for download in Site Properties, this content type is called Reputation Settings. ■ Revocation Data (downloaded by default, not configurable from Symantec Endpoint Protection Manager) ■ Symantec Whitelist ■ Submission Control signatures ■ Auto-Protect portal list ■ Power Eraser definitions ■ Extended File Attributes and Signatures ■ Endpoint Detection and Response ■ Common Network Transport Library and Configuration ■ Advanced Machine Learning
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. ■ Centralized Reputation Settings ■ Revocation Data ■ Symantec Whitelist ■ 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 ■ Power Eraser definitions ■ Extended File Attributes and Signatures ■ Endpoint Detection and Response ■ Common Network Transport Library and Configuration

Table 9-6 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. ■ Centralized Reputation Settings ■ Revocation Data ■ Symantec Whitelist ■ Submission Control signatures ■ Auto-Protect Portal List ■ Power Eraser Definitions ■ Extended File Attributes and Signatures ■ Endpoint Detection and Response ■ Common Network Transport Library and Configuration ■ Advanced Machine Learning
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. ■ Centralized Reputation Settings ■ Revocation Data ■ Symantec Whitelist ■ Submission Control signatures ■ Auto-Protect Portal List ■ Power Eraser Definitions ■ Extended File Attributes and Signatures ■ Endpoint Detection and Response ■ Common Network Transport Library and Configuration
Proactive Threat Protection > SONAR	SONAR Definitions Submission Control signatures Extended File Attributes and Signatures Advanced Machine Learning
Proactive Threat Protection > Application Control	Submission Control signatures Extended File Attributes and Signatures Application Control content (as of 14.2)

Table 9-6 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
Integrations policy	WSS Traffic Redirection (as of 14.0.1 MP1)
Network and Host Exploit Mitigation > Intrusion Prevention	■ 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 ■ Extended File Attributes and Signatures
Network and Host Exploit Mitigation > Firewall	Submission Control signatures Extended File Attributes and Signatures
Host Integrity	Host Integrity content Submission Control signatures Extended File Attributes and Signatures

See "Downloading content from LiveUpdate to the Symantec Endpoint Protection Manager" on page 186.

See "How to update content and definitions on the clients" on page 178.

See "Choose a distribution method to update content on clients" on page 179.

See "Reverting to an older version of the Symantec Endpoint Protection security updates" on page 213.

Configuring clients to download content from an internal LiveUpdate server

By default, your Windows clients get their updates from the management server. If you select the default management server and your environment includes Mac and Linux computers, Mac and Linux clients get their updates from the default LiveUpdate server.

If you manage a large number of clients, you may want to use Group Update Providers (GUPs) for Windows clients. 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 215.

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.
  For more information about using an internal LiveUpdate server, refer to the *LiveUpdate Administrator's Guide*.

  Note: Symantec Endpoint Protection Manager no longer includes legacy support for LiveUpdate Administrator 1.x. To continue using an internal LiveUpdate server, you should upgrade to the latest version of LiveUpdate Administrator. Support for LiveUpdate Administrator 2.x and later is always enabled.

- Use the LiveUpdate Settings policy to configure your clients to use that internal LiveUpdate server.

Note: 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 201.

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:
     Domain name: http://myliveupdateserver.com
     IPv4 address: http://192.168.133.11/Export/Home/LUDepot
     IPv6 address: http://[fd00:fe32::b008]:80/update

- If you use the LAN method, type the server UNC path name. For example, \\myliveupdateserver\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 to client computers" on page 202.

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 204.

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:
  Domain name: http://myliveupdateserver.com
  IPv4 address: http://192.168.133.11/Export/Home/LUDepot
  IPv6 address: http://[fd00:fe32::b008]:80/update

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 Under **Mac Settings**, click **Advanced Settings**.

If you want to let client computers get product update settings through LiveUpdate, click **Download Symantec Endpoint Protection product updates using a LiveUpdate server**.

10 Click **OK**.

To configure Linux 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 **Linux 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:
  Domain name: http://myliveupdateserver.com
  IPv4 address: http://192.168.133.11/Export/Home/LUDepot
  IPv6 address: http://[fd00:fe32::b008]:80/update

6 If your server uses FTP or HTTPS, click **Advanced Server Settings**.

7 Select the FTP or HTTPS mode that the server uses, and then click **OK**.

8 Click **OK**.

See "Randomizing content downloads from a LiveUpdate server" on page 207.

See "Configuring Windows client updates to run when client computers are idle" on page 208.

See "Choose a distribution method to update content on clients" on page 179.

Configuring clients to download content from an external LiveUpdate server

By default, Symantec Endpoint Protection Manager provides updates to Windows clients. To help mitigate network overloads for Windows client updates, you should also let clients get updates from a LiveUpdate server. Linux and Mac clients must get updates from a LiveUpdate server, or you can set up the Apache web server as a reverse proxy to download updates from the management server.

See "Choose a distribution method to update content on clients" on page 179.

Enabling Mac and Linux clients to download LiveUpdate content using the Apache Web server as a reverse proxy

---

Note: You may also want to 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 200.

To configure clients to download content from an external LiveUpdate server

1. In the console, open a LiveUpdate policy, and click **Edit**
2. Under **Windows Settings**, **Mac Settings**, or **Linux Settings**, click **Server Settings**.
3. Click **Use the default Symantec LiveUpdate server** or specify another LiveUpdate server. If needed, specify your proxy configuration.
4. Click **OK**.

See "How to update content and definitions on the clients" on page 178.

Configuring Symantec Endpoint Protection Manager to connect to a proxy server to access the Internet and download content from Symantec LiveUpdate

You can configure Symantec Endpoint Protection Manager to go through a proxy server to connect to the Internet. 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 "Specifying a proxy server that clients use to communicate to Symantec LiveUpdate or an internal LiveUpdate server" on page 201.

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.

Note: You configure proxy settings for other client communications separately.

To specify a proxy server that clients on Windows or computers or Linux 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** or under **Linux Settings**, click **Server Settings**.
5. Under **LiveUpdate Proxy Configuration**, click **Configure Proxy Options**.
6. Do one of the following:
   - For Windows clients, on the **HTTP or HTTPS** tab, select the desired options. You can also specify proxy settings for FTP.
   - For Linux clients, on the **HTTP** 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**.

See "How to update content and definitions on the clients" on page 178.

Configuring the LiveUpdate download schedule to client computers

The LiveUpdate client schedule settings are defined in the LiveUpdate Settings policy. These settings apply to LiveUpdate sessions that get the latest updates from either a Symantec LiveUpdate server or an internal LiveUpdate server.

See "Configuring clients to download content from an external LiveUpdate server" on page 200.

See "Configuring clients to download content from an internal LiveUpdate server" on page 196.

To save bandwidth, you can let your clients run scheduled LiveUpdate sessions only if either of the following conditions is met:

- Virus and spyware definitions on a client computer are more than 2 days old.
- A client computer is disconnected from Symantec Endpoint Protection Manager for more than 8 hours.

Note: To make sure that any client computers that connect to your network infrequently get the latest updates, let these computers get updates from a Symantec LiveUpdate server. These servers are public, and the client therefore does not depend on a connection to your network to get updates.

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 Make sure that **Enable LiveUpdate Scheduling** is checked. This option is enabled by default.

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 any additional options, if required. Symantec recommends that you keep the default values for running LiveUpdate if the definitions are out of date, or if the client has not connected recently to the management server.

8 Click **OK**.

See "Randomizing content downloads from a LiveUpdate server" on page 207.

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.

To configure the schedule for LiveUpdate downloads to Linux client computers

1 On the **LiveUpdate Settings Policy** tab, right-click the policy that you want, and then click **Edit**.

2 Under **Linux Settings**, click **Schedule**.

3 Check **Enable LiveUpdate Scheduling**. This option is enabled by default.

Note: You should not uncheck this box. If you disable **LiveUpdate Scheduling**, Linux clients do not get the latest updates.

---

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 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.

You can also randomize content downloads.

6 Click **OK**.

See "How to update content and definitions on the clients" on page 178.

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 installation file. 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 Click **OK**.

See "Reverting to an older version of the Symantec Endpoint Protection security updates" on page 213.

See "Configuring the LiveUpdate download schedule to client computers" on page 202.

Mitigating network overloads for client update requests

You must manage your networks for the critical but infrequent situation when too many clients simultaneously request a full set of virus and spyware definitions from the management server or from a Group Update Provider. This situation can occur if the management server encounters an error or runs out of disk space, so that the download and update of the definitions on the client then fails. This situation can also occur if the management server does not download a definitions package and a client then requests this specific delta. In either case, the client then must request a package with a full set of definitions from either the management server or from the Group Update Provider.

To help prevent overloads on your network, the management server provides the following features:

- A notification when the management server receives a specified number of requests for a full set of definitions within a specified period of time.
  You set the conditions for this notification based on what constitutes an overload for your environment. To configure the notification, add a **Network load: requests for virus and spyware full definitions** notification condition.
  See "Setting up administrator notifications" on page 671.
- The ability to let clients get deltas for virus and spyware definitions from a LiveUpdate server if the management server can provide only a full set. In a LiveUpdate Settings policy, click **Advanced Settings** > **Download smaller client installation packages from a LiveUpdate server**.
- The ability to block clients from downloading a full set of virus and spyware definitions from the management server.
  If you receive a notification of a network overload, you can block any further downloads of full packages from the management server. You cannot, however, stop any downloads that are already in progress. Configure this option by clicking **Admin** > **Servers** > *server_name* > **Edit the server properties** > **Full Definitions Download** > **Prevent clients from downloading full definition packages**.

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 "Randomizing content downloads from the default management server or a Group Update Provider" on page 206.

See "Randomizing content downloads from a LiveUpdate server" on page 207.

See "Configuring clients to download content from an internal LiveUpdate server" on page 196.

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 207.

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 205.

See "Configuring clients to download content from an internal LiveUpdate server" on page 196.

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 on Windows or Linux clients. 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 206.

To randomize 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**, **Mac Settings**, or **Linux 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 205.

See "Configuring clients to download content from an internal LiveUpdate server" on page 196.

Configuring Windows client updates to run when client computers are idle

To ease Windows 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 Windows 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 to client computers" on page 202.

See "Configuring Windows client updates to run when definitions are old or the computer has been disconnected" on page 209.

Configuring Windows client updates to run when definitions are old or the computer has been disconnected

You can ensure that Windows 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 Windows 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 Manager for more than:** and then set the number of minutes or hours.

7 Click **OK**.

See "Configuring the LiveUpdate download schedule to client computers" on page 202.

See "Configuring Windows client updates to run when client computers are idle" on page 208.

Configuring clients to download content from the Symantec Endpoint Protection Manager

The default method for downloading content to clients is by using the management server.

You do not define the schedule for the updates from the management server to the clients. The clients download content from the management server based on the communication mode and heartbeat frequency.

To configure clients to download content from the Symantec Endpoint Protection Manager

1. In the console, open a LiveUpdate policy, and click **Edit**
2. Under **Windows Settings**, click **Server Settings**.
3. Make sure that **Use the default management server** is checked.
4. Click **OK**.

See "Updating policies and content on the client using push mode or pull mode" on page 165.

Testing engine updates before they release on Windows clients

Symantec Endpoint Protection contains several engines that carry out parts of its functionality. These engines are binary files (.dll or .exe) and are delivered with the security definitions. Symantec updates the functionality of these engines to enhance Symantec Endpoint Protection's capabilities and to respond to new threats.

While Symantec updates virus definitions several times a day, the engine content is updated on a quarterly basis. Symantec provides the engine updates using LiveUpdate.

As of version 14.0.1 MP1, Symantec provides a special server lets you download and test the engine content before you roll out the content to your production environment. Symantec releases these updates on the Early Adopter server (EAS). Engine updates are released a few weeks before the engines are available for general release on the public LiveUpdate server.

You download the engine updates using the EAS, try them in a lab environment, and let Symantec know of any conflicts you encounter. This process lets Symantec fix these conflicts ahead of the general release.

Use the following process to test engine updates:

Step 1: Create a group of test computers to receive content

Step 2: Configure test computers to receive prereleased content from the Early Adopter server

Step 3: Configuring test and non-test computers to a particular engine version

Step 4: Set up notifications for new engine releases (optional)

Step 5: Monitor the test computers after engine content is released

Step 1: Create a group of test computers to receive content

The most accurate test of engine compatibility is with the production systems that do real work. Create a permanent testing group by selecting a set of client computers to receive EAS content using the following criteria:

- Identify the various types of critical systems within your environment. These systems may vary from each other by hardware, software, or function. For example, you might identify retail systems such as a gold desktop image, point-of-sale systems, and web servers, among other critical systems to test.
- Use multiple systems of each type as some software conflicts may manifest only intermittently. Choose the production systems that already have the installed software that you normally use and that perform a representative load of work.
- Configure the test client computers that receive the early release content like the production computers that you do not test. Both the clients that you test and do not test should have the same Symantec Endpoint Protection features installed and use the same policies.

If you prefer not to use production computers for testing with the EAS, you may use lab-based systems. In this case, you may want to write the automation that exercises the functions of the systems under test and simulate load.

For customers with a small number of client computers, all you need is one Symantec Endpoint Protection Manager and one Symantec Endpoint Protection for Windows client.

Step 2: Configure test computers to receive prereleased content from the Early Adopter server

For the test group, configure LiveUpdate to download the content from the Symantec Early Adopter server by performing the following steps.

To configure a site to download content from the Symantec Early Adopter LiveUpdate server

1. In the console, click **Admin** > **Servers**.
2. Under **Servers**, right-click **Local Site**, and then click **Edit Site Properties**.
3. Under **LiveUpdate Source Servers**, click **Edit Source Servers**.
4. In the **LiveUpdate Servers** dialog box, click **Use the Symantec LiveUpdate server for prereleased content**, and then click **OK** > **OK**.

To configure the managed clients to use the prerelease Symantec Early Adopter LiveUpdate server

1. In the console, open a new LiveUpdate Settings policy, and click **Policies** > **LiveUpdate**.
2. Under **Windows Settings**, click **Server Settings** > **Use a LiveUpdate server** > **Use the Symantec LiveUpdate server for prereleased content**.
3. Click **OK**, and assign the policy to the test group.

As long as your LiveUpdate Settings policy gets content from the EAS, the test clients continue to receive the prereleased versions of the content.

Note: For non-test groups, keep the LiveUpdate Settings policy configured to the LiveUpdate server that you normally use. After the engines are available for general release, all client computers receive LiveUpdate content, depending on how you configured your client computers to receive it.

See "Configuring clients to download content from an internal LiveUpdate server" on page 196.

See "Configuring clients to download content from an external LiveUpdate server" on page 200.

Step 3: Configuring test and non-test computers to a particular engine version

Configure several LiveUpdate Content policies so that:

- The test group receives the latest version of the security definitions and engines. This group downloads all future content revisions with the prerelease engine version in it.
- The non-test groups receive an existing, safe version of the engine.
  Starting in 14.0.1 MP1, you can also lock on an engine version. With this option, clients continue to receive the latest security definitions that are associated with a particular engine, but not the latest engine version.
  See "Reverting to an older version of the Symantec Endpoint Protection security updates" on page 213.
  After you are satisfied that the test group functions normally with the prereleased content, you manually choose the next engine version for these non-test groups.

Step 4: Set up notifications for new engine releases (optional)

To get notifications for planned engine releases that LiveUpdate downloads to the Symantec Endpoint Protection Manager, do one of the following tasks:

- Add a notification for when new content has been downloaded to Symantec Endpoint Protection Manager. Starting in 14.0.1 MP1, notifications for new content include new engine releases as well as security definitions. You receive notifications only if one or more

LiveUpdate Content policies that specify a content revision by engine version are locked due to an available engine update.

To view notifications, on the **Home** page, in the **Security Status** pane, click **View Notifications**.

Note: Updates on the EAS are as frequent as on the regular LiveUpdate server. If you feel that you receive these notifications too often, configure the notifications to not appear.

See "Setting up administrator notifications" on page 671.

- For earlier releases, log on to the Customer Subscription Portal.
  How PCS Customers can Sign Up for Alerts and Notifications

Step 5: Monitor the test computers after engine content is released

After Symantec publishes an engine update to the EAS, begin monitoring the computers that you configured to receive this content. Monitor the following items:

- Verify that the test computers run the prerelease version of the engine updates.
  Verifying which engine and definitions run on the client computers
- Uptime and available resources on the servers and other critical infrastructure using tools such as Microsoft System Center Operations Manager.
- The applications that run on the client computers to ensure that they continue to perform as expected.
- The Symantec Endpoint Protection client status to ensure that it remains connected to the management server and is protected.
  See "Checking whether the client is connected to the management server and is protected" on page 163.

In addition, run the client after you modify the policies or run a scan to ensure that the computer functions as expected.

If you notice any unexpected behavior or suspect a software conflict exists with the engine update, contact Support for assistance. Usually, if Symantec confirms that there is a software conflict before the beginning of the phased rollout, Symantec reschedules the publishing, and works with you to correct the issue. Symantec then republishes an updated engine to EAS.

Reverting to an older version of the Symantec Endpoint Protection security updates

By default, the latest version of content that is downloaded from a LiveUpdate server to the management server is automatically downloaded to Windows clients. The LiveUpdate Content policy specifies the type of content that clients are permitted to check for and install.

However, you may need to download an older version of the content in the following cases:

- The latest set of definitions or engine causes a software conflict on the client computers.
- You want time to test new engines on control groups before the content releases into production.

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 revert to an older version of the Symantec Endpoint Protection security updates

1. In the console, click **Policies** > **LiveUpdate**, and open a LiveUpdate Content policy.
2. Under **Windows Settings**, click **Security Definitions**.

   You cannot roll back content for Mac clients or Linux clients.
3. To roll back the content to a specific version, click one of the following options:
   - **Select a revision** > **Edit**, and select the revision number.
     This option locks the clients to one particular set of security definitions. The clients do not receive any new security definitions.
   - **Select an engine version** > **Edit**, and then select the engine version.
     As of 14.0.1 MP1, this option locks the clients to one particular engine, but continues to distribute the latest security definitions that are associated with that engine. Select the engine version if you know the current engine works in your environment, and you need to test a newer engine in a different group before you release it. Or, click **Use latest available** for clients to continually receive the latest engine version and definitions for that content type. 14.0.1 and earlier clients ignore this setting.
4. Click **OK**.

   You do not need to restart the client computer for the content to update.
5. After you resolved any troubleshooting issues, under **Windows Settings**, click **Security Definitions** > **Use latest available** for each content type.

See "Testing engine updates before they release on Windows clients" on page 210.

See "Downloading content from LiveUpdate to the Symantec Endpoint Protection Manager" on page 186.

Using Group Update Providers to distribute content to clients

A Group Update Provider (GUP) is a client computer that distributes content updates directly to other clients.

Advantages of the GUPs include:

- They conserve bandwidth and management server resources by offloading processing power to the GUP.
- They deliver updates effectively to clients with limited or slow network connectivity.
- They are easier to set up than an internal LiveUpdate server.

Table 9-7 Tasks to use Group Update Providers

Step	Description
Step 1: Understand the differences between the types of Group Update Providers that you can configure	You can set up single, multiple, or cross-subnet Group Update Providers. The type of Group Update Provider that you set up depends on your network and the clients on that network. The types of Group Update Provider are not mutually exclusive. You can configure one or more types of Group Update Provider per policy. See "About the types of Group Update Providers" on page 216. See "About the effects of configuring more than one type of Group Update Provider in your network" on page 221.
Step 2: Verify client communication	Before you configure Group Update Providers, verify that the client computers 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 connectivity problems between Symantec Endpoint Protection Manager and the Symantec Endpoint Protection client" on page 765.
Step 3: Configure Group Update Providers in one or more LiveUpdate Settings policies	You configure Group Update Providers in the LiveUpdate Settings policy. See "Configuring clients to download content from Group Update Providers" on page 219.

Table 9-7 Tasks to use Group Update Providers *(continued)*

Step	Description
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 or location" on page 321.
Step 5: Verify that clients are designated as Group Update Providers	To view the client computers that are designated as Group Update Providers, do one of the following tasks: ■ Click **Clients** > **Clients** tab > right-click the client, and then click **Edit Properties**. The Group Update Provider field is **True** or **False**. ■ See "Searching for the clients that act as Group Update Providers" on page 221.

About the types of Group Update Providers

You can configure several types of Group Update Providers in a LiveUpdate Settings policy. The types of Group Update Providers that you use depend on how your network is set up. You can configure one or more types of Group Update Provider per policy; they are not mutually exclusive.

Table 9-8 When to use a particular type of Group Update Provider

Group Update Provider Type	When to use
Single	A single Group Update Provider is a dedicated client computer that provides content for one or more groups of clients. Configuring a single Group Update Provider turns a single client into a Group Update Provider. A single Group Update Provider can be a client computer in any group. Use a single Group Update Provider when you want to use the same Group Update Provider for all your client computers. You use a single LiveUpdate Settings policy to specify a static IP address or host name for a single Group Update Provider. However, if the client that serves as a single Group Update Provider changes location, you must change the IP address in the policy. If you want to use different single Group Update Providers in different groups, you must create a separate LiveUpdate Settings policy for each group.
Multiple	Multiple Group Update Providers use a set of rules, or criteria, to elect themselves to serve groups of clients in their own subnets. All client computers are on the same subnet. You specify the criteria that client computers must meet to qualify as a Group Update Provider. If a client computer meets the criteria, the management server adds the client to a global list of Group Update Providers. The management server 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. Configuring multiple Group Update Providers turns multiple clients into Group Update Providers. Use multiple Group Update Providers for any of the following scenarios: ■ 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.

Table 9-8 When to use a particular type of Group Update Provider *(continued)*

Group Update Provider Type	When to use
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. An explicit Group Update Providers list does not turn clients into Group Update Providers. When you configure an explicit list, you can specify that the clients with IP addresses that fall on a particular subnet should use a particular Group Update Provider. A client may have multiple IP addresses, and the management server considers all of the client's IP addresses when it matches which 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 management server 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.

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 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 Group Update Providers the clients with this policy should use for content updates.
  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.

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.

See "About the effects of configuring more than one type of Group Update Provider in your network" on page 221.

See "Using Group Update Providers to distribute content to clients" on page 215.

See “Configuring clients to download content from Group Update Providers” on page 219.

See “Downloading content from LiveUpdate to the Symantec Endpoint Protection Manager” on page 186.

Configuring clients to download content from Group Update Providers

You use the LiveUpdate Settings policy so that clients get updates from the Group Update Provider only and never from the management server. You can set up single, multiple, or cross-subnet Group Update Providers. The type of Group Update Provider that you set up depends on your network and the clients on that network.

See “About the types of Group Update Providers” on page 216.

To configure clients to download content from Group Update Providers

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.
   - Follow the steps in To configure an explicit list of Group Update Providers.
9. Under **Group Update Provider Settings**, 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, check **Single Group Update Provider IP address or host name**, and 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.
2. Return to the procedure to configure a Group Update Provider.

To configure multiple Group Update Providers

1. In the **Group Update Provider** dialog box, check **Multiple Group Update Providers**, and then click **Configure Group Update Provider List**.
2. In the **Group Update Provider List** dialog box, select the tree node **Group Update Provider**, and then click **Add** to add a rule set.
3. 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**
4. If you selected **Computer IP Address or Host Name** or **Registry Keys**, click **Add**.
5. Type or select the IP address or host name, Windows registry key, or operating system information.

   Click **Help** for information on configuring rules.
6. Click **OK** until you return to the **Group Update Provider List** dialog box, where you can optionally add more rule sets.
7. Click **OK**.
8. Return to the procedure to configure a Group Update Provider.

To configure an explicit list of Group Update Providers

1. In the **Group Update Provider** dialog box, check **Explicit Group Update Providers for roaming clients**, and then click **Configure Explicit Group Update Provider List**.
2. Click **Add**.
3. In the **Add Explicit Group Update Provider** dialog box, type the client subnet that you want to map these Group Update Providers to.

   Click **Specify Client Subnet Mask** to add multiple client subnets at one time.
4. 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.

   Type in the necessary settings for the type of mapping you selected.
5. Click **OK**.

See “Choose a distribution method to update content on clients” on page 179.

See “Using Group Update Providers to distribute content to clients” on page 215.

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 215.

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, this file is:

64-bit operating systems: `C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\data\outbox\agent\gup\globallist.xml`

32-bit operating systems: `C:\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.

See "About the types of Group Update Providers" on page 216.

See "Configuring clients to download content from Group Update Providers" on page 219.

Using Intelligent Updater files to update content on Symantec Endpoint Protection clients

Symantec recommends that client computers use LiveUpdate to update content on Symantec Endpoint Protection clients. 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 for Windows are designed to update the clients only. Intelligent Updater files do not contain the information that Symantec Endpoint Protection Manager needs to update its managed clients.

The Intelligent Updater file for Windows is a self-executing file that contains virus and spyware definitions. Additional Intelligent Updater files are available for SONAR definitions, and for intrusion prevention signatures. For Mac and for Linux, you can download virus and spyware definitions.

After you download the file, you can use your preferred distribution method to distribute the updates to your clients.

Note: An Intelligent Updater file does not provide updates for any other type of content. For example, Intelligent Updater does not support the extended file attributes and signatures, the Auto-Protect portal list, Power Eraser definitions, or reduced-size definitions.

To download an Intelligent Updater file

1. Using your web browser, go to the following page:

   https://www.symantec.com/security_response/definitions.jsp

2. From the drop-down list, select one of the available Symantec Endpoint Protection options:
   - Symantec Endpoint Protection 12.1

(Windows and Linux)

- Symantec Endpoint Protection 12.1.2 (Windows and Linux)
- Symantec Endpoint Protection 12.1.3 (or later) (Windows and Linux)
- Symantec Endpoint Protection 14 (Windows and Linux)
- Symantec Endpoint Protection for Macintosh 12.x
- Symantec Endpoint Protection for Macintosh 14.x

The page refreshes to display the content available for that version.

3 Under **File-Based Protection (Traditional Antivirus)**, **Network-Based Protection (IPS)** (Windows only), or **Behavior-Based Protection** (Windows only), next to **Download** click **Definitions**.

4 Click the appropriate file name for the version of the client you want to update.

Note: For Linux virus definitions, click the **Unix Platforms** tab.

5 When you are prompted for a location in which to save the file, select a folder on your hard drive.

6 Distribute the file to the client computers using your preferred distribution method.

You can repeat the procedure if you need additional files.

To install the virus definitions and security updates files on a client computer

1 On the client computer, locate the Intelligent Updater file that was distributed to the client.

2 Do one of the following:

- For Windows: Double-click the .exe file, and then follow the on-screen instructions.
- For Mac: Double-click the .zip file, double-click the .pkg file, and then follow the on-screen instructions.
- For Linux: Verify that the file has executable permissions, verify that uudecode and uncompress are installed, and then run the .sh file with superuser privilege. See the following for more information:
  How to update a Linux-based computer with Intelligent Updater definitions

See “Choose a distribution method to update content on clients” on page 179.

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 and Linux clients can only receive content updates from internal or external LiveUpdate servers.

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 9-9 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 "Downloading content from LiveUpdate to the Symantec Endpoint Protection Manager" on page 186. See "How to update content and definitions on the clients" on page 178.
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 226.
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 226.
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 by default in subfolders under the *SEPM_Install*\data\outbox\agent folder. To update clients, you need to use the index2.dax files. The default location for *SEPM_Install* is C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager. See "Downloading content from LiveUpdate to the Symantec Endpoint Protection Manager" on page 186. See "Distributing the content using third-party distribution tools" on page 227.

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:

- Vista and later operating systems
  C:\ProgramData\Symantec\Symantec Endpoint Protection\CurrentVersion\inbox
- Pre-Vista operating systems (for legacy 12.1.x clients)
  C:\Documents and Settings\All Users\Application Data\Symantec\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 "Configuring clients to download content from an internal LiveUpdate server" on page 196.

Preparing unmanaged clients to receive updates from third-party distribution tools

If you install unmanaged clients from the installation file, 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:

- Vista and later operating systems
  C:\ProgramData\Symantec\Symantec Endpoint Protection\CurrentVersion\inbox
- Pre-Vista operating systems (for legacy 12.1.x clients)
  C:\Documents and Settings\All Users\Application Data\Symantec\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 add one of the following Windows registry keys:
   - On 12.1.5 and later clients on a 64-bit computer, add **HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Symantec\Symantec Endpoint Protection\SMC\SPE\TPMState**
   - On 12.1.5 and later clients on a 32-bit computer, and all other 12.1 clients, add **HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\SMC\SPE\TPMState**
2. Set the value type of the registry key to DWORD (32-bit) or QWORD (64-bit) and the value to hexadecimal 80 as follows:

   ```
   0x00000080 (128)
   ```

3. Save the registry key, and then exit the registry editing tool.

See “Using third-party distribution tools to update client computers” on page 225.

See “Distributing the content using third-party distribution tools” on page 227.

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 downloads” on page 191.

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. By default, the ContentInfo.txt file is located in C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\Inetpub\content\.

For example, you might see the following entry:

```
{535CB6A4-441F-4e8a-A897-804CD859100E}: SEPC Virus Definitions
Win32 12.1 RU6 - 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. By default, the folders for client groups are found in C:\Program Files (x86)\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="D5ED508E8CF7A8A4450B0DBA39BCCB25" DeltaFlag="1"
FullSize="625203112" LastModifiedTime="1425983765211" Moniker=
"{535CB6A4-441F-4e8a-A897-804CD859100E}" Seq="150309034"/>
```

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.

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:

   SEPM_Install\data\outbox\agent

   Where *SEPM_Install* represents the installation folder for Symantec Endpoint Protection Manager. The default installation folder is C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager.
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:

   SEPM_Install\Inetpub\content

   Where *SEPM_Install* represents the installation folder for Symantec Endpoint Protection Manager. The default installation folder is C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager.
8. Open and read `ContentInfo.txt` to discover the content that each *target moniker* folder contains.

   The contents of each directory are in the following format: *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 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.

11 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 225.

See "Preparing unmanaged clients to receive updates from third-party distribution tools" on page 226.

Downloading Endpoint Protection security patches to Windows clients

What are security patches and how do they work?

A security patch is a software patch for Symantec Endpoint Protection clients that corrects a vulnerability that exists in the client code. As new vulnerabilities become known, Symantec delivers a security patch to fix the vulnerability and uploads it to a LiveUpdate server. Starting in version 14, you can download security patches from the LiveUpdate server to the management server. You then download the patches to clients in the same way as other content, using a LiveUpdate server, the management server, or a Group Update Provider (GUP).

Note: In versions earlier than 14, security patches are only available as part of a new release, and only as part of a client deployment package using AutoUpgrade. In 14, you can use AutoUpgrade to install the security patches on the clients when both Symantec Endpoint Protection Manager and the clients have the same version installed.

Security patches are not available for 12.1.x clients.

See "Choose a distribution method to update content on clients" on page 179.

If the client and the management server versions match, the clients can get the security patches from a LiveUpdate server, a management server, or a GUP. If the client and the management server versions do not match, the clients get the security patches from a LiveUpdate server only, as in the case when a management server manages clients with multiple versions. If you want to use the management server or a GUP to download patches, you must update either the client or the management server version so that they are the same version.

In addition, the language for the client must match the management server. For example, a French management server that manages French, German, and simplified Chinese clients provides security patches to the French clients only.

See "Upgrading client software with AutoUpgrade" on page 156.

Note: A security patch is not the same as a Maintenance Patch. A security patch only addresses a possible security issue, and is delivered through LiveUpdate. A Maintenance Patch provides other updates, such as to offer support for new operating systems, and is delivered as a full installation download through MySymantec.

About Endpoint Protection release types and versions

Table 9-10 displays examples of whether or not the client can receive security patches from the management server, based on the version number of Symantec Endpoint Protection Manager and the Symantec Endpoint Protection client.

Table 9-10 Examples of which client versions download which security patches

Management server version	Client version	Does the client download patches from the management server?
14.2	14.2	Yes
14.2	14.0.1 MP2	No
14.0.1 MP2	14.0.1 MP2	Yes
14.0.1 MP2	14.0.1 MP1	No
14.0.1 MP2	14.2	No

Installing security patches on Windows clients

By default, LiveUpdate downloads security patches to Symantec Endpoint Protection Manager, which in turn installs the patches on the clients based on the distribution method you have configured for the other content types.

After a client downloads and installs a security patch, it continues to run the previous, unpatched version of the client until the client is restarted. You must restart the client to run the latest

patch. Either the client end user must restart the computer, or you must run the restart command from the management server. The management server sends you a notification that indicates which clients require a restart.

To install security patches on Windows clients

1. In the console, verify that LiveUpdate is configured to download the security patches to the management server.

   In the **Content Types to Download** dialog box, make sure that **Client security patches** is checked.

   See "Downloading content from LiveUpdate to the Symantec Endpoint Protection Manager" on page 186.

2. To run a report to find out which release is installed on the client computers, run a **Protection Content Versions** report.

   See "Generating a list of the Symantec Endpoint Protection versions installed in your network" on page 630.

3. Verify that the LiveUpdate Settings policy is configured to download the patches to the clients.

   In a LiveUpdate Settings policy, under **Windows Settings**, click **Advanced Settings**. Make sure **Download security patches to fix the vulnerabilities in the latest version of the Symantec Endpoint Protection client** is checked.

   See "Reverting to an older version of the Symantec Endpoint Protection security updates" on page 213.

4. When notified, restart the client computers.

   See "Restarting the client computers from Symantec Endpoint Protection Manager" on page 127.

Section 3

Managing groups, clients, and administrators

Chapter 10

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.

If you rename **My Company** in the cloud console, the group name does not change in Symantec Endpoint Protection Manager.

Table 10-1 Group management actions

Task	Description
Add groups	See "How you can structure groups" on page 236. See "Adding a group" on page 237.
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 237.
Disable inheritance for subgroups	The subgroups inherit the same security settings from the parent group by default. You can disable inheritance. See "Disabling a group's inheritance" on page 242.
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 263. 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 272.
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 318. See "Assigning a policy to a group or location" on page 321. See "Performing the tasks that are common to all policies" on page 313.
Perform 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 243. See "Blocking client computers from being added to groups" on page 243.

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.
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 groups, 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.

Best Practices for Creating Group Structure

See “Performing the tasks that are common to all policies” on page 313.

See “Managing groups of clients” on page 234.

Adding a group

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

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

Note: You cannot add groups to the Default Group.

See "How you can structure groups" on page 236.

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	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 238. See "Connecting Symantec Endpoint Protection Manager to a directory server" on page 239. See "Connecting to a directory server on a replicated site" on page 240.

Table 10-3 Importing existing groups and computers *(continued)*

Step	Description
Step 2: Import either entire organizational units or containers	You can import the existing group structure from Active Directory or LDAP into the Symantec Endpoint Protection Manager. You can also copy individual accounts from an imported group structure into an existing Symantec Endpoint Protection Manager group structure. See "Importing organizational units from a directory server" on page 241.
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 237. See "Assigning a policy to a group or location" on page 321. See "The types of security policies" on page 316.
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 "Choosing the authentication method for administrator accounts" on page 283. See "Checking the authentication to a directory server" on page 292.

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 239.

See "Importing existing groups and computers from an Active Directory or an LDAP server" on page 237.

See "Importing organizational units from a directory server" on page 241.

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 241.

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 739.

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 239.

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 add all accounts within an organizational unit or container to Symantec Endpoint Protection Manager, then you must still import it. Once the import completes, you copy the accounts that you want to manage to existing client groups.

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 239.
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 237.

See "About importing organizational units from the directory server" on page 238.

Disabling 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.

Policies that come from the cloud do not follow the Symantec Endpoint Protection Manager policy inheritance configuration. Instead, they follow the inheritance rules that are defined in the cloud.

See "Managing groups of clients" on page 234.

To disable 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, uncheck **Inherit policies and settings from parent group "*group name*"**.

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 135.

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 243.

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 with Communication Update Package Deployment" on page 173.

To move a client computer to another group

1. In the console, click **Clients**.
2. On the **Clients** page, 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 234.

Chapter 11

Managing clients

This chapter includes the following topics:

Managing client computers

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 "Searching for the clients that do not have the client software installed" on page 248. ■ 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 256. ■ You can add a client to a group and install the client software later. See "Choosing a method to install the client using the Client Deployment Wizard" on page 119.
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 "Checking whether the client is connected to the management server and is protected" on page 163. See "Symantec Endpoint Protection client status icons" on page 165. 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 "How does the client computer and the management server communicate?" on page 168.
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 161. You can troubleshoot any connection issues. See "Troubleshooting communication problems between Symantec Endpoint Protection Manager and the console or the database" on page 773.

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 client computers" on page 247. See "Checking whether the client is connected to the management server and is protected" on page 163. ■ 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 625. ■ 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 249.
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 316. See "How Symantec Endpoint Protection technologies protect your computers" on page 28. ■ You can require a password on the client. See "Password-protecting the Symantec Endpoint Protection client" on page 260.
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 243. 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
Decide whether users should have control over computer protection (optional)	You can specify the kind of control that users have over the protection on client computers. ■ For Virus and Spyware Protection, Proactive Threat Protection, and Memory Exploit Mitigation, you can lock or unlock a check box within the policies to specify whether users can change individual settings. ■ 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 "Preventing users from disabling protection on client computers" on page 327. ■ If users need full control of the client, you can install an unmanaged client. See "How does the client computer and the management server communicate?" on page 168.
Remove the Symantec Endpoint Protection client software from decommissioned computers (optional)	If you decommissioned a client computer and you want to use the license for a different computer, you can uninstall the Symantec Endpoint Protection client software. For the managed clients that do not connect, Symantec Endpoint Protection Manager deletes clients from the database after 30 days by default. You can change the period of time after which Symantec Endpoint Protection Manager deletes the client from the database. By deleting a client, you also save space in the database. See "Uninstalling the Symantec Endpoint Protection client for Windows" on page 132. See "Uninstalling the Symantec Endpoint Protection client for Mac" on page 133. See "Uninstalling the Symantec Endpoint Protection client for Linux" on page 134. See "Purging obsolete clients from the database to make more licenses available" on page 102.

Viewing the protection status of 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.
- 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 any clients that run an earlier version of Symantec Endpoint Protection, 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 "Checking whether the client is connected to the management server and is protected" on page 163.

See "Running commands on client computers from the console" on page 253.

See "Searching for the clients that do not have the client software installed" on page 248.

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.

Searching for the clients that do not have the client software installed

You can search for clients in a group based on the following criteria:

- Client software is installed.
- Clients run on Windows, Mac, or Linux computers
- Windows clients are in computer mode or user mode.
- Clients are non-persistent and offline in Virtual desktop infrastructures.

See "Viewing the protection status of client computers" on page 247.

See "Checking whether the client is connected to the management server and is protected" on page 163.

To search for the clients that 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 **New users or computers that have been created but that don't yet have the client software installed**.
5. 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. You can find out which client computers in the Finance group need the latest virus definitions installed.

Note: To search for most of the information about the users, you must collect user information either 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 259.

To search for information about client computers

1. In the console, click **Clients**.
2. Under **Tasks**, click **Search clients**.
3. In the **Search clients** dialog box, in the **Find** drop-down list, click either **Computers** or **Users**.
4. Click **Browse** to select a group other than the default group. Click to select the group, and then click **OK**.
5. 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.

   To find embedded clients, you can search for the type of write filters in use. Click **Enhanced Write Filter**, **File Based Write Filter**, or **Unified Write Filter** to search for whether they are installed, enabled, or both. You can also search for the reduced-size client. Click **Install Type** to search for a value of **Reduced Size**.

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

You can use standard Boolean operators in your search criteria. Click **Help** for more information on the options.

7 In the **Value** cell, type the search string.

8 Click **Search**.

You can export the results into a text file.

9 Click **Close**.

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

See "Viewing the protection status of client computers" on page 247.

What are the commands that you can run on client computers?

You can run commands remotely on individual clients or an entire group from the console.

To see the results of any of the commands, click **Monitors** page > **Logs** > **Command Status**. You can also run some of the commands from the **of type** drop-down list.

System administrators and domain administrators can run these commands automatically. For limited administrators, you enable or disable access for each command individually.

See "Adding an administrator account and setting access rights" on page 282.

See "Running commands on client computers from the console" on page 253.

Table 11-2 Commands that you can run on client computers

Commands	Description
Analyze (cloud console)	Runs the **Analyze** command from the cloud console. The **Analyze** command shows the progress of all requests that you submitted for analysis from the cloud console to the Content Analysis System (CAS). Configuring Symantec Endpoint Protection to use the Symantec Content Analysis System
Cancel Evidence of Compromise Scan	Starts or cancels a scan that you use on third-party remote monitoring and management.

Table 11-2 Commands that you can run on client computers *(continued)*

Commands	Description
Scan	Runs an 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 436.
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 "Downloading content from LiveUpdate to the Symantec Endpoint Protection Manager" on page 186.
Update Content and Scan	Updates content by initiating a LiveUpdate session and runs an on-demand scan on client computers.
Start Power Eraser Analysis	Runs a Power Eraser analysis on the selected computers. You should typically run Power Eraser only on a single computer or a small number of computers. You should only run Power Eraser when computers exhibit instability or have persistent problems. Unlike other scans, Power Eraser does not automatically remediate any potential threats. You must review the detections in the logs and specify which risks you want to remove or leave alone. **Note:** Mac and Linux client computers do not process this command. See "Starting Power Eraser analysis from Symantec Endpoint Protection Manager" on page 788.
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** page. **Note:** Restart options apply only to Windows client computers. Mac client computers always perform a hard restart. Linux client computers ignore this command. See "Restarting the client computers from Symantec Endpoint Protection Manager" on page 127. **Note:** You can ensure that a Windows 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 254.

Table 11-2 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. Symantec recommends that you always keep Auto-Protect enabled. You can lock the setting so that users on client computers cannot disable Auto-Protect. See "Customizing Auto-Protect for Windows clients" on page 468. See "Customizing Auto-Protect for Mac clients" on page 470. If Auto-Protect for email is disabled, you enable it 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:** Linux client computers do not process this command. See "Managing firewall protection" on page 336.
Enable Download Insight and **Disable Download Insight**	Enables or disables Download Insight on the client computers. **Note:** Mac and Linux client computers do not process this command. See "Managing Download Insight detections" on page 442.
Delete From Quarantine	Deletes all files from Quarantine. This command only appears on the **Risk** log > **Action** drop-down list. How to delete Quarantined items from the Symantec Endpoint Protection Manager
Collect file fingerprint list	Generates a non-editable file fingerprint list from the selected clients. The collected fingerprint list appears on the **Policies** tab under **Policy Components** > **File Fingerprint Lists**. Typically, you run this command on a single computer or small group of computers. If you select multiple computers, the command collects a separate list for each computer. **Note:** Mac and Linux client computers do not process this command.
Place Client(s) in Quarantine and **Remove Client(s) From Quarantine**	Lets you add clients to or remove clients from Quarantine. These commands are only available when you enable Deception.

See "Symantec Endpoint Protection features based on platform (12.1.x through 14.x)" on page 795.

Running commands on client computers from the console

You can manually run commands on the client computer at any time, such as starting or canceling a scan. On managed clients, the commands that you run from the management server override the commands that the user runs. The order in which commands are processed on the client computer differs from command to command. Regardless of where the command is initiated, the commands are processed in the same way.

See "What are the commands that you can run on client computers?" on page 250.

You run these commands from the following locations:

- The **Clients** page.
- The **Computer Status** log. You can run the **Cancel All scans** and **Start Power Eraser Analysis** commands from the **Computer Status** log only.
- The **Risk** Log. You can run the **Delete from Quarantine** command from the **Risk** log only. How to delete Quarantined items from the Symantec Endpoint Protection Manager

If you start a scan, you can also cancel it immediately.

To run commands on the client computer from the Clients page

1. In the console, click **Clients**.
2. Do one of the following actions for groups or computers:
   - In the left pane, right-click the group, and then click **Run a command on the group > *command***
   - Click the **Clients** tab, right-click the computers, and then click **Run command on computers > *command***
3. In the message that appears, click **Yes**.

To run a command from the Computer Status log

1. Click **Monitors** > **Logs** > the **Computer Status** log type, and then click **View Log**.
2. Select a command from the **Command** list box, select the computers, and then click **Start**.

Note: You can cancel an in-progress scheduled scan or a scan that you started by clicking **Cancel All Scans** from the command list.

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 the command results

1. Click **Monitors**.
2. On the **Command Status** tab, select a command in the list, and then click **Details**.

Note: You can also cancel a scan in progress by clicking the **Cancel Scan** icon in the **Command** column of the scan command.

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 Windows client between user mode and computer mode

You add Windows 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. Linux clients and Mac clients are only installed in 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 256.
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. If you import your existing group structure into Symantec Endpoint Protection Manager from Microsoft Active Directory or LDAP directory servers to organize clients by user, use user mode. 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. See "Importing existing groups and computers from an Active Directory or an LDAP server" on page 237.

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 Windows 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.

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 the following traffic to the network to let other computers know of the device's presence:

- Address Resolution Protocol (ARP) traffic (ICMPv4)
- Neighbor Discovery Protocol (NDP) traffic (ICMPv6)

A client that is enabled as an unmanaged detector collects and sends this packet information to the management server. The management server searches the 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 client computers from the console” on page 253.
- Switch the client to computer mode.
  See “Switching a Windows client between user mode and computer mode” on page 254.
- Install the client on a computer that runs all the time.

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.

Preventing and allowing users to change the client's user interface

What can users change on the client user interface?

You as the administrator set the user control level to determine whether the user can make changes to the client. For example, you can prevent the user from opening the client user interface or the notification area icon. The user interface features that you manage for the users are called managed settings. The user does not have access to all of the client features, such as password protection.

See "Password-protecting the Symantec Endpoint Protection client" on page 260.

How do I configure 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.

Note: Most of these settings apply to the Windows client only. You can configure a few options on the Mac client in server control only.

To configure user interface settings in mixed control

1 Click **Clients > Policies** tab.

  See "Preventing users from disabling protection on client computers" on page 327.

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 some of the options that you set to **Server**, click the **Client User Interface Settings** tab to configure them:

  For information on where in the console you configure the remaining options that you set to **Server**, click **Help**. For example, to enable firewall settings, configure them in the Firewall policy.

  See "Enabling communications for network services instead of adding a rule" on page 372.

  See "Enabling network intrusion prevention or browser intrusion prevention" on page 383.

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 server control.

   See "Preventing users from disabling protection on client computers" on page 327.
2. In the **Client User Interface Settings** dialog box, check the options that you want to appear on the client.
3. Click **OK**.
4. Click **OK**.

See "Configuring firewall settings for mixed control" on page 371.

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 135.

To collect user information

1. In the console, click **Admin**, and then click **Install Packages**.
2. In the **Install Packages** pane, click **Client Install Packages**.
3. Under **Tasks**, click **Set User Information Collection**.
4. In the **Set User Information Collection** dialog box, check **Collect User Information**.
5. In the **Pop-up Message** text box, type the message that you want users to read when they are prompted for information.
6. 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.
7. 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.

8 In the Optional column, check the check box next to any fields that you want to define as optional for the user to complete.

9 Click **OK**.

Password-protecting the Symantec Endpoint Protection 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 service.
- Uninstall the client.
  As of 14.0.1, you can require Mac users to type a password to uninstall the client.
- Import and export the client communication settings.

See "Preventing and allowing users to change the client's user interface" on page 257.

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 **Password**.

4 In the **Client Password Settings** window, check any or all of the check boxes.

  If the boxes are grayed out, this group inherits policies from a parent group. Before you can proceed, you must either edit the policy in the parent group or disable inheritance for this group.

  See "Disabling a group's inheritance" on page 242.

5 In the **Password** and **Confirm password** text boxes, type the same password.

  You can create a password that is between 6 to 256 characters in length.

  If you see a message that the password strength is not acceptable, consider increasing the strength of your password. However, you may still be able to save the password.

  Check **Apply password settings to non-inherited sub groups** to modify the password protection settings for any child group that does not inherit its settings from a parent. This setting appears for a parent group only.

6 Click **OK**.

Chapter 12

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 234.
Set up locations for groups of remote clients	See "Managing locations for remote clients" on page 263.
Configure communication settings for locations	See "Configuring communication settings for a location" on page 272.
Strengthen your security policies	See "About strengthening your security policies for remote clients" on page 273.
Turn on client notifications	See "About turning on notifications for remote clients" on page 274.

Table 12-1 Managing remote clients *(continued)*

Task	Description
Customize client log management settings	Customize the log settings for remote clients, especially if clients are offline for several days. To reduce bandwidth and the load on your management servers, make the following changes: ■ Set clients to not upload their logs to the management server. ■ Set clients to upload only the client security logs. ■ Set 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 virus and spyware event data.
Monitor remote clients	See "About monitoring remote clients from the management server" on page 275. See "Monitoring roaming Symantec Endpoint Protection clients from the cloud console" on page 276.

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
- 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 234. You may find the following examples helpful: See "Setting up Scenario One location awareness conditions" on page 268. See "Setting up Scenario Two location awareness conditions" on page 270.

Table 12-2 Location awareness tasks that you can perform *(continued)*

Tasks	Description
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 265.
Add locations	You can add locations to groups. See "Adding a location to a group" on page 266.
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 267.
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 272.

See the article Best Practices for Symantec Endpoint Protection Location Awareness.

See "Managing remote clients" on page 261.

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 263.

See “Adding a location to a group” on page 266.

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 234.

See "About strengthening your security policies for remote clients" on page 273.

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 263.

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 for which you want to add a location.
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 for which you want to add a location.
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 for which you want to add a location.
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 270.

See "Managing remote clients" on page 261.

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.

Symantec suggests 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 for which you want to add a location.

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 for which you want to add a location.

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 268.

See "Managing remote clients" on page 261.

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 "Updating policies and content on the client using push mode or pull mode" on page 165.

See "Managing locations for remote clients" on page 263.

See "Managing groups of clients" on page 234.

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 261.

Best practices for Firewall policy settings for remote clients

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 340.

See "Enabling communications for network services instead of adding a rule" on page 372.

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 261.

About monitoring remote clients from the management server

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.

Table 12-4 Displays to monitor remote client security *(continued)*

Display	Description
Monitors > Summary Type > Network Threat Protection	Displays the information about attack types and sources.

See "Managing remote clients" on page 261.

See "Monitoring roaming Symantec Endpoint Protection clients from the cloud console" on page 276.

Monitoring roaming Symantec Endpoint Protection clients from the cloud console

Roaming Symantec Endpoint Protection clients are the clients that intermittently connect to the management server. Roaming clients access the Internet at different locations, such as airports, hotels, or at other companies, where they are at higher risk. Symantec Endpoint Protection Manager provides on and off-network protection for these client computers using location awareness.

In 14.1 and earlier, roaming clients send critical events to the management server only when they are connected. As of 14.2, roaming clients automatically send critical events to the cloud console when the clients cannot connect to the management server. After the roaming client reconnects to the management server, the clients send any new critical events on the management server. The client is also no longer considered to be roaming.

Use the list of critical events as a way to strengthen the security policies on the Symantec Endpoint Protection Manager. For example, suppose Employee1's client has a higher number of denial-of-service attacks when Employee1 is located in a particular hotel. Therefore, you can create a location for that hotel and enable denial of service detections in the Firewall policy.

What are the critical events that the cloud console displays?

See "About monitoring remote clients from the management server" on page 275.

Location awareness best practices for Endpoint Protection

Finding roaming clients and critical events

To find out which clients are roaming, look for the following items:

- Whether the device is connected directly to the cloud console and not the management server.
- The location as defined in the Symantec Endpoint Protection Manager location awareness policy
- The external IP address of the client.

To find roaming clients and critical events

1. In the cloud console, go to **Alerts and Events**.
2. On the **Security Events** tab, under **Connection Type**, click **Cloud** to display the events that the client sends to the cloud console.

   To display events that the management server sends, click **Symantec Endpoint Protection Manager**.
3. Under **Severity**, click **Critical**.

   The cloud console filters and displays only the critical security events that the roaming clients detected.
4. To find the location and external IP address, select the device and look for the Device Location entry.

What are the critical events that the cloud console displays?

The roaming client uploads the following security events to the cloud console:

- Port scan events
- Mac spoofing
- Denial of service
- Canary
- IPS
- Deception
- Memory Exploit Mitigation
- Host Integrity compliance

The roaming client uploads the following security events to the cloud console:

- Antivirus
- SONAR

Chapter 13

Managing administrator accounts and passwords

This chapter includes the following topics:

Managing administrator accounts

You can use administrator accounts to manage Symantec Endpoint Protection Manager datacenters. Administrators log on to Symantec Endpoint Protection Manager 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 and one domain. For a large company with multiple sites and Windows domains, you most likely need multiple administrators, some of whom have more access rights than others. You may also need to add multiple domains within Symantec Endpoint Protection Manager.

You manage domains and administrator accounts and their passwords on the **Admin** page.

Table 13-1 Account administration

Task	Description
Decide whether to add multiple domains	Decide whether to add domains. See "About domains" on page 307. See "Adding a domain" on page 308. See "Switching to the current domain" on page 309.
Add administrator accounts	Add accounts for administrators who need access to the Symantec Endpoint Protection Manager console. **1** Add the types of administrator accounts that you need, and the level of access rights. See "About administrator accounts and access rights" on page 281. See "Adding an administrator account and setting access rights" on page 282. **2** Choose a method to authenticate administrator for when they log on to Symantec Endpoint Protection Manager (optional). By default, the Symantec Endpoint Protection Manager database authenticates the administrator's credentials. See "Choosing the authentication method for administrator accounts" on page 283.

Table 13-1 Account administration *(continued)*

Task	Description
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. If an administrator is locked out of their account, they must wait the specified time before logging on again. You cannot unlock an account during the lockout interval. See "Unlocking an administrator's account after too many logon attempts" on page 304.
Change and reset lost passwords	■ Change the password for your account or another administrator's account. See "Changing the password for an administrator account or the embedded database" on page 296. ■ Reset a lost password using the **Forgot your password?** link that appears on the management server logon screen. The administrator receives an email that contains a link to activate a temporary password. See "Resetting a forgotten Symantec Endpoint Protection Manager password" on page 297. See "Displaying the Forgot your password? link so that administrators can reset lost passwords" on page 299. ■ Allow administrators to save their user name and password on the management server logon screen. See "Displaying the Remember my user name and Remember my password check boxes on the logon screen" on page 301. ■ Force the administrator's logon password to expire after a certain number of days. See "Displaying the Remember my user name and Remember my password check boxes on the logon screen" on page 301.
Configure logon options for Symantec Endpoint Protection Manager	You can configure the following logon 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 to the Symantec Endpoint Protection Manager console" on page 301. ■ 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 302. ■ Changing how long an administrator can stay logged on to the management server. See "Changing the timeout period for staying logged on to the Symantec Endpoint Protection Manager console" on page 304. See "Logging on to the Symantec Endpoint Protection Manager console" on page 48.

About administrator accounts 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 Protection 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 13-2 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.

Table 13-2 Administrator roles and responsibilities *(continued)*

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. ■ Cannot administer licenses. Only system administrators can administer licenses. See "About domains" on page 307.
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 "Adding an administrator account and setting access rights" on page 282.

See "Managing administrator accounts" on page 279.

Adding an administrator account and setting access rights

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** > **Administrators**.
2. Under **Tasks**, click **Add an administrator**.
3. In the **Add Administrator** dialog box, on the **General** tab, enter the user name and email address.
4. On the **Access Rights** tab, specify the type of administrator account.

   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 cannot log on to the management server.

   See "About administrator accounts and access rights" on page 281.
5. On the **Authentication** tab, under **Symantec Endpoint Protection Manager Authentication**, type the password the administrator should use to log on.

   When the administrator logs on to the Symantec Endpoint Protection Manager, Symantec Endpoint Protection Manager verifies with the database that the user name and password are correct.

   See "Choosing the authentication method for administrator accounts" on page 283.
6. Click **OK**.

Choosing the authentication method for administrator accounts

You can choose from several authentication methods that the management server uses to check administrators' credentials before they log on.

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.

Table 13-3 Authentication methods

Type	When to use
Symantec Endpoint Protection Manager authentication (default)	Authenticates the administrators with the administrator's user name and password that 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. You can display the **Password never expires** option so that an administrator's account does not expire. See "Enabling Symantec Endpoint Protection Manager logon passwords to never expire" on page 299.
Two-factor authentication	Authenticates the administrators with Symantec VIP authentication on their smartphone. Administrators provide a unique, one-time verification code when they log on, in addition to a password. For this option to be available, you must first add the appropriate PKCS keystore file and keystore's password. See "Configuring two-factor authentication with Symantec VIP" on page 288.
RSA SecurID authentication	Authenticates the administrators by a using RSA SecurID token (not software RSA tokens), RSA SecurID card, or RSA keypad card (not RSA smart cards). To authenticate administrators who use an RSA SecurID mechanism, first install the RSA Authentication Manager server and enable encrypted authentication for RSA SecurID. See "Using RSA SecurID authentication with Symantec Endpoint Protection Manager" on page 285.
Directory server authentication	Authenticates the administrators with an LDAP server or the Microsoft Active Directory server. 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. Synchronization with LDAP servers is not supported. See "Connecting Symantec Endpoint Protection Manager to a directory server" on page 239. See "Checking the authentication to a directory server" on page 292.

Table 13-3 Authentication methods *(continued)*

Type	When to use
Smart card authentication	Authenticates the administrators who work as civilians or military personnel in U.S. Federal Agencies and who must use a PIV card or CAC to log on. See "Configuring Symantec Endpoint Protection Manager to authenticate administrators who log on with smart cards" on page 289.

To choose an authentication method for administrator accounts

1. Add an administrator account.

   See "Adding an administrator account and setting access rights" on page 282.
2. On the **Authentication** tab, select the authentication method if you do not want to use **Symantec Endpoint Protection Manager Authentication** (default).
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.

Using RSA SecurID authentication with Symantec Endpoint Protection Manager

Note: In an IPv6 environment, you must install and enable the IPv4 stack on the Symantec Endpoint Protection Manager server to use RSA SecurID authentication.

Configure RSA SecurID to authenticate Symantec Endpoint Protection Manager administrators

If you want to authenticate administrators who use the Symantec Endpoint Protection Manager with RSA SecurID, you must first enable encrypted authentication by configuring a connection to an RSA Authentication Manager server.

To configure RSA SecurID to authenticate Symantec Endpoint Protection Manager administrators

1. Install an RSA Authentication Manager server, if necessary. Use RSA Authentication Manager 8.1.
2. Install and properly configure the RSA Authentication Agent on the Symantec Endpoint Protection Manager server to connect to the RSA server. Use RSA Authentication Agent 7.x.

   See the section called "Configure RSA SecurID to authenticate Symantec Endpoint Protection Manager administrators" on page 285.
3. Ensure that the Symantec Endpoint Protection Manager server registers as a valid host on the RSA Authentication Manager server.
4. Ensure that the `sdconf.rec` file on the RSA Authentication Manager 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 Authentication Manager 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, an administrator needs a logon name, the token (hardware), and a PIN.

Install the RSA Authentication Agent and configure the Symantec Endpoint Protection Manager server to use RSA SecurID authentication

To use RSA SecurID with Symantec Endpoint Protection Manager, you must install the RSA Authentication Agent on the Symantec Endpoint Protection Manager server and configure it as a SecurID Authentication client.

To install the RSA Authentication Agent

1. Install the software for the RSA Authentication Agent on the Symantec Endpoint Protection Manager server. You can install the software by running the Windows .msi file from the RSA Authentication Agent installation file or CD.
2. Copy the `sdconf.rec` file from the RSA Authentication server to the Symantec Endpoint Protection Manager server.

   For earlier versions of RSA Authentication Agent, copy `nodesecret.rec`, `sdconf.rec`, and `agent_nsload.exe`.

To configure the Symantec Endpoint Protection Manager server to use RSA SecurID authentication

1. Log on to the Symantec Endpoint Protection Manager console, and then click **Admin > Servers**.
2. Under **Servers**, under **Local Site**, click the management server.
3. Under **Tasks**, click **Configure SecurID authentication**.
4. In the **Welcome to the Configure SecurID Authentication Wizard** panel, click **Next**.
5. In the **Qualification** panel of the **Configure SecurID Authentication Wizard** panel, read the prerequisites and verify that you meet them all.
6. Click **Next**.
7. 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.
8. Click **Next**, and then click **Test** to test your configuration.
9. In the **Test Configuration** dialog box, type the user name and password for your SecurID, and then click **Test**.

   It now authenticates successfully.

Add Symantec Endpoint Protection Manager administrators that use RSA SecurID authentication

To add Symantec Endpoint Protection Manager administrators that use RSA SecurID authentication

1. Add an administrator account.

   See "Adding an administrator account and setting access rights" on page 282.
2. On the **Authentication** tab, click RSA SecurID Authentication.

   If this option is unavailable, review the configuration guidelines.

   See the section called "Configure RSA SecurID to authenticate Symantec Endpoint Protection Manager administrators" on page 285.
3. Click **OK**.

You can also change an existing administrator account to use RSA SecurID authentication, though this practice is not recommended, especially for default administrator account, admin. If you provide invalid information when you edit an existing user, it is more difficult to recover that user.

However, if you modify an existing administrator account, 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.

See "Choosing the authentication method for administrator accounts" on page 283.

Configuring two-factor authentication with Symantec VIP

If you use Symantec VIP two-factor authentication in your environment, you can configure Symantec Endpoint Protection Manager administrators to authenticate with it.

Two-factor authentication adds an extra layer of security to the logon process. When two-factor authentication is enabled, you must provide a unique, one-time verification code when you log on, in addition to a password. You can receive the code by voice, text, or with the free Symantec VIP Access app. This app is recommended because it is the most secure and it is easy to use. For a quick overview of Symantec VIP, see:

Symantec VIP: Enterprise-grade authentication made easy for everyone

You manage the individual two-factor authentication settings for each individual administrator that uses Symantec Endpoint Protection Manager Authentication. Administrators that authenticate with RSA SecurID or Directory authentication cannot use two-factor authentication.

Note: Two-factor authentication is not supported over IPv6, or in a FIPS-enabled environment.

To configure Symantec Endpoint Protection Manager for two-factor authentication with Symantec VIP

1. In the console, click **Admin > Servers**, and then click the local server name.
2. Under **Tasks**, click **Configure VIP authentication**.
3. Browse to the PKCS keystore file to select it, enter the keystore's password, and then click **OK**.

   The certificate automatically propagates to other Symantec Endpoint Protection Manager consoles in the same site without the need for replication. You do not need to manually add the certificate to each Symantec Endpoint Protection Manager on the site.

   To propagate the certificate to a Symantec Endpoint Protection Manager on a different site, the sites must be replication partners.

To configure the administrator for two-factor authentication with Symantec VIP

1. Verify that the Symantec Endpoint Protection Manager administrator has a corresponding user name on the Symantec VIP Manager that matches exactly, including case sensitivity. The passwords for the two user names do not have to match.

   Consult Symantec VIP Manager documentation for how to configure a user name.

   Symantec VIP Access Manager 3.0 Administrator's Guide
2. In the console, click **Admin > Servers > Administrators**.
3. Select an existing administrator, and then click **Edit the administrator**.

   You can also add a new administrator to configure.
4. On the **Authentication** tab, click **Enable two-factor authentication using VIP**.

Configuring Symantec Endpoint Protection Manager to authenticate administrators who log on with smart cards

As of version 14.2, administrators who work for US Federal Agencies can log on to Symantec Endpoint Protection Manager using a smart card.

To set up smart card authentication, the administrator needs to perform the following steps:

Step 1: Configure Symantec Endpoint Protection Manager for smart card authentication

Step 3: Add an administrator account and register the smart card

Step 3: Add an administrator account and register the smart card

Step 4: Log on to Symantec Endpoint Protection Manager using a smart card

About smart cards

The United States Federal Agencies now use a software system that allows smart card authentication for the HSPD-12 requirements. A U.S. Federal smart card contains the necessary data for the cardholder to be granted access to Federal facilities and information systems. This access ensures appropriate levels of security for all applicable Federal applications.

Some Windows client computers or workstations already have PIV or CAC readers built into the keyboards.

Symantec Endpoint Protection Manager authenticates administrators who use the following types of smart cards:

- Personal identity verification (PIV) card (for civilians)
- Common Access Card (CAC) (for military personnel)
- In FIPS mode: Symantec Endpoint Protection Manager does not support smart cards that are signed using ECDSA and RSASSA-PSS.

- In non-FIPS mode: Symantec Endpoint Protection Manager does not support smart cards that are signed using RSASSA-PSS.

See: HSPD-12

Step 1: Configure Symantec Endpoint Protection Manager for smart card authentication

This step validates that the card certificate is issued by the correct authority. Then, at the point that the administrator logs on, the management server reads the smart card's certificate and validates it against these CA certificates.

To validate a certificate file, the management server checks that the certificate file is not listed in a certificate revocation list (CRL) on the Internet.

Make sure that all the root files and intermediate files are present on the administrators' computer, or else they cannot log on.

To configure Symantec Endpoint Protection Manager for smart card authentication

1. In the console, click **Admin > Servers**, and select the local management server name.
2. Under **Tasks**, click **Configure Smart Card Authentication**.
3. In the **Specify the paths for the root and/or intermediate certificate files** text box, browse to one or more certificate files, and then click **OK**.

   Select all the certificate files you need to check for revocation. To select multiple files, press **Ctrl**.

   Note: Optional: If the management server that the administrator logs on to cannot access the Internet, in the **Specify the paths for the certificate revocation lists** text box, and add a .crl or a .pem file. You must also perform the following task on these management servers. Step 2 (Optional): Configure the management server to perform the revocation check (Required for dark networks)

4. Click **OK**.
5. If the administrator logs on to Symantec Endpoint Protection Manager remotely with the web console, they must restart the Symantec Endpoint Protection Manager service and the Symantec Endpoint Protection Manager Web service.

   See “Stopping and starting the management server service” on page 151.

Step 2 (Optional): Configure the management server to perform the revocation check (Required for dark networks)

If a management server does not have Internet access, you must configure it to check for the CRL file on the management server computer instead. Without this check, administrators can

still log on, but the management server cannot check the CRL file, which can cause security issues.

To configure the management server to perform the revocation check (dark networks only)

1. On this management server, open the following file: *Symantec Endpoint Protection Manager installation path*\tomcat\etc\conf.properties
2. In the `conf.properties` file, add **smartcard.cert.revocation.ocsp.crldp.enabled=false** and save the file.
3. Restart the management server service.

   See "Stopping and starting the management server service" on page 151.

Step 3: Add an administrator account and register the smart card

This step authenticates the administrators as the user of the smart card by setting up PIV authentication. PIV authentication requires a certificate and key pair that is used to verify that the PIV credential was issued by an authorized entity, has not expired, and has not been revoked. The PIV credential also identifies the administrator the same individual it was issued to.

This step also ensures that users only need to enter their user name, insert the card, and type the smart card pin to log on to Symantec Endpoint Protection Manager. They do not need to enter a Symantec Endpoint Protection Manager password.

Note: Smart card authentication is not supported over IPv6.

To add an administrator account and register the smart card

1. In the console, click **Admin > Servers > Administrators**.
2. Add a new administrator or edit an existing administrator.

   See "Adding an administrator account and setting access rights" on page 282.
3. On the **Authentication** tab, click **Enable smart card authentication**.
4. Browse to the authentication certificate file for the PIV card or CAC for that administrator, and then click **OK**.
5. In the **Confirm Change** dialog box, type the administrator's password and click **OK**.

Follow this step for each administrator that uses a smart card to log on to Symantec Endpoint Protection Manager.

Step 4: Log on to Symantec Endpoint Protection Manager using a smart card

To log on to Symantec Endpoint Protection Manager, the administrator inserts the card into a smart card reader and types a pin number. The smart card must always be inserted into the reader while the smart card administrator is logged on and using the management server. If the administrator removes the smart card, the Symantec Endpoint Protection Manager logs off the administrator within 30 seconds.

The Java console and web console support smart card authentication. The RMM console and the REST API do not support smart card authentication.

See "Logging on to the Symantec Endpoint Protection Manager console" on page 48.

Troubleshooting and replication

If two sites replicate each other, the site with the most recently configured CA file overwrites the CA file on all other sites.

See the section called "How does replication work?" on page 742.

Checking the authentication to a directory server

You can check that an Active Directory or LDAP server authenticates the user name and password for an administrator account that you create. The check evaluates whether you added the user name and password correctly, and whether or not the account name exists on the directory server.

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.

You can also check 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 **Check 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 13-4 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).
Step 2	Add multiple administrator accounts	You add multiple system administrator accounts. The account for anonymous access does not have a user name or password. See "To add the administrator accounts using the directory server entries" on page 294.

To add the directory server connections to check 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 and setting access rights" on page 282.

See "Choosing the authentication method for administrator accounts" on page 283.

2 After you add each administrator account and click the **Check Account** option, you see a message. In some cases, the message appears to invalidate the account information. The administrator can still log on to Symantec Endpoint Protection Manager, however.

Administrator account 1:

- On the **General** tab, enter 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 **Check Account**.
  The system administrator `john` can log on to Symantec Endpoint Protection Manager with directory authentication.

Administrator account 2:

- On the **General** tab, enter 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 **Check Account**.
  The system administrator `john` cannot log on into Symantec Endpoint Protection Manager with directory authentication.

Administrator account 3:

- On the **General** tab, enter 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 **Check 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, enter 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 **Check 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 239.

Changing the password for an administrator account or the embedded database

Changing the password for an administrator account

You need to change the password for your account or another administrator's account if the password is forgotten, lost, or compromised.

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.

If you change the password to fix an administrator account lockout, the administrator must still wait for the lockout period to expire.

Note: The password must contain at least 8 characters and fewer than 16 characters. It must include at least one lowercase letter [a-z], one uppercase letter [A-Z], one numeric character [0-9], and one special character ["/ \ [ ] : ; | = , + * ? < >].

See "Unlocking an administrator's account after too many logon attempts" on page 304.

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**.

   Press `F1` to see the password restrictions.
3. Type both your password and the administrator's new password.
4. Click **Change**.

See "Resetting a forgotten Symantec Endpoint Protection Manager password" on page 297.

See "Displaying the Forgot your password? link so that administrators can reset lost passwords" on page 299.

Changing the embedded database password

When you configure the management server and 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 automatically. As of 14, you can change the database password by rerunning the Management Server Configuration Wizard and reconfiguring Symantec Endpoint Protection Manager.

To change the embedded database password

1. On the Windows **Start** menu, navigate to **Symantec Endpoint Protection Manager** > **Symantec Endpoint Protection Manager Tools** > **Management Server Configuration Wizard**.
2. Click **Reconfigure the management server**, and then click **Next** > **Next**.

   See "Reinstalling or reconfiguring Symantec Endpoint Protection Manager" on page 756.
3. Click **Default Embedded database** > **Change the database administrator password**, and type the new password.
4. Follow the instructions in each panel to finish the configuration

Resetting a forgotten Symantec Endpoint Protection Manager password

If you have a system administrator account, you can reset your own password and allow other administrators to reset their own passwords.

To reset a lost password, make sure that the following items are enabled:

- Administrators can reset their own passwords.
  See "Displaying the Forgot your password? link so that administrators can reset lost passwords" on page 299.

- The **Forgot your password?** link is set to appear on the management server logon screen. By default, this link appears.
  See "Displaying the Remember my user name and Remember my password check boxes on the logon screen" on page 301.
- The mail server must be configured so that the mail server sends the notification.
  To troubleshoot Symantec Endpoint Protection Manager email failure, see Sending test email messages fails in Endpoint Protection Manager console.
  See "Establishing communication between the management server and email servers" on page 668.

Use this method for the administrator accounts that authenticate by using Symantec Management Server authentication but not by either RSA SecurID authentication or directory authentication.

Note: The password must contain at least 8 characters and fewer than 16 characters. It must include at least one lowercase letter [a-z], one uppercase letter [A-Z], one numeric character [0-9], and one special character ["/ \ [ ] : ; | = , + * ? < >].

See "Choosing the authentication method for administrator accounts" on page 283.

To reset a forgotten Symantec Endpoint Protection Manager password

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.
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**.

   The administrator receives an email that contains a link to activate a temporary password. An administrator can request a temporary password from the management console only once per minute. For security reasons, the management server does not verify the entries.
5. The administrator must change the temporary password immediately after logging on.

To verify whether the administrator successfully reset the password, check that the administrator received the email message.

See "Changing the password for an administrator account or the embedded database" on page 296.

When you cannot reset your password

If you cannot recover your administrator password with the **Forgot your password?** functionality, Symantec cannot assist with the recovery of your password. You must reconfigure the Symantec Endpoint Protection Manager and database without a database backup. This procedure overwrites the previous management server and database settings and enables you to recreate a new password. Therefore, it is critical that you configure your email settings correctly when you set up the management server and when you audit administrator account information.

See "Restoring the database" on page 759.

See Reinstalling or reconfiguring Symantec Endpoint Protection Manager.

Displaying the Forgot your password? link so that administrators can reset lost passwords

If you have a system administrator account, you can enable other administrators to reset their forgotten passwords. You enable a **Forgot your password?** link on the Symantec Endpoint Protection Manager logon screen so that administrators can request a temporary password.

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 "Resetting a forgotten Symantec Endpoint Protection Manager password" on page 297.

See "Displaying the Remember my user name and Remember my password check boxes on the logon screen" on page 301.

Enabling Symantec Endpoint Protection Manager logon passwords to never expire

If you use Symantec Endpoint Protection Manager authentication, the default option for passwords is set to expire after 60 days.

For 12.1.5 and later, you can display an option for administrators to use a password that never expires. This option is disabled by default to increase security, so you must enable it first. After

you enable the option, the option appears on the **Authentication** tab for an administrator account.

To enable Symantec Endpoint Protection Manager logon passwords to never expire

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, click **Allow never expiring passwords for administrators**.
6. Click **OK**.
7. Click **Admin** > **Administrators**, and open the administrator account.
8. On the **Authentication** tab, click **Password never expires**, and then click **OK**.

See "Resetting a forgotten Symantec Endpoint Protection Manager password" on page 297.

See "Unlocking an administrator's account after too many logon attempts" on page 304.

About accepting the self-signed 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 article, How to install the certificate for Endpoint Protection Manager for Web console access.

See "Logging on to the Symantec Endpoint Protection Manager console" on page 48.

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

You can create and display a customizable message that all administrators see before they can log on to the console. The main 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 and click **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 standalone web browser that is connected to the management server.

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

1. In the console, click **Admin**, and then click **Domains**.
2. Select the domain for which you want to add a logon banner.
3. Under **Tasks**, click **Edit Domain Properties**.
4. On the **Logon Banner** tab, check **Provide a legal notice to administrators when they log on to Symantec Endpoint Protection Manager**.
5. Type the banner title and text.

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

See "Adding an administrator account and setting access rights" on page 282.

Displaying the Remember my user name and Remember my password check boxes on the logon screen

A system administrator can enable the **Remember my user name** and **Remember my password** check boxes to appear on the Symantec Endpoint Protection Manager logon screen for another administrator account. The administrator's user name and password are 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 "Resetting a forgotten Symantec Endpoint Protection Manager password" on page 297.

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 and 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 and setting access rights" on page 282.

See "Logging on to the Symantec Endpoint Protection Manager console" on page 48.

Unlocking an administrator's account after too many logon attempts

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 for 15 minutes after five failed attempts.

You cannot unlock the administrator account without waiting for the specified period of time to pass. However, you can disable the administrator account from locking, though this action does not unlock the account. You can also change the number of unsuccessful logon attempts and wait the time that is permitted before the account is locked. A password change does not reset or otherwise affect the lockout interval.

For added security in 12.1.5 and later, after the first lockout the lockout interval doubles with each additional lockout. Symantec Endpoint Protection Manager reinstates the original lockout interval after a successful logon occurs or after 24 hours pass since the first lockout. For example, if the original lockout interval is 15 minutes, the second lockout triggers a 30-minute lockout interval. The third lockout triggers a 60-minute lockout interval. If the first lockout occurs at 2:00 P.M. on Thursday, then the 24-hour period ends 2:00 P.M. Friday, and Symantec Endpoint Protection Manager resets the lockout interval to 15 minutes.

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

1. In the console, click **Admin** > **Administrators**.
2. Under **Administrators**, select the administrator account that is locked.
3. Under **Tasks**, click **Edit the administrator**.
4. On the **General** tab, uncheck **Lock the account after the specified number of unsuccessful logon attempts**.

See “Resetting a forgotten Symantec Endpoint Protection Manager password” on page 297.

See “Changing the password for an administrator account or the embedded database” on page 296.

See “Enabling Symantec Endpoint Protection Manager logon passwords to never expire” on page 299.

Changing the timeout period for staying logged on to the Symantec Endpoint Protection Manager console

To help protect Symantec Endpoint Protection Manager, the console requires you to enter your user name and password again after one hour. To increase security, you can decrease the timeout period before you must log on to the management console again.

This logon timeout period applies to when you log on to the management console locally or through the remote Java console. The logon timeout period for the remote web console is based on the shortest timeout value that you define. For example, you set the **Site Properties** settings to 60 minutes, the Apache settings to 30 minutes, and the browser settings to 10 minutes. The console then times out after 10 minutes.

To change the timeout period for staying logged on to the Symantec Endpoint Protection Manager local or remote Java 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 one of the available options for length of time.
4. Click **OK**.

To change the timeout period in Apache Tomcat for staying logged on to the Symantec Endpoint Protection Manager remote web console

1. On the server that runs Symantec Endpoint Protection Manager, open the following file in a text editor:

   `*Program Files*\Symantec\Symantec Endpoint Protection Manager\tomcat\etc\conf.properties`

2. Add the following line, if it is not present:

   scm.web.timeout.minutes=*timeout_value*

   The value *timeout_value* is the number of minutes of inactivity after which the console logs out. The maximum value is 60. A value of 0 has the same effect as not adding the line at all.

   If this line is present, you can change the timeout value.

3. Save and close the file.
4. For your changes to take effect, open the Windows Services (services.msc) and restart the Symantec Endpoint Protection Manager service.

To change the timeout period in Internet Explorer for staying logged on to the Symantec Endpoint Protection Manager remote web console

- Follow the instructions in the Microsoft article, How to change the default keep-alive time-out value in Internet Explorer, to change the registry key HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\InternetSettings.

To change the timeout period in Mozilla Firefox for staying logged on to the Symantec Endpoint Protection Manager remote web console

1. In the address bar, enter the following:

   `about:config`

2. Click to acknowledge the warning.
3. Search for the following line:

   network.http.keep-alive.timeout

4. Change the value (in seconds) to the one that you want. The default is 115.

Note: Google Chrome does not have configurable settings for the network timeout period.

See "Logging on to the Symantec Endpoint Protection Manager console" on page 48.

Chapter 14

Managing domains

This chapter includes the following topics:

About domains

When you install a management server, the Symantec Endpoint Protection Manager console includes one domain, which is called Default. Domains are a logical separation of data that is separate from the Symantec Endpoint Protection Manager infrastructure. 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.

The primary purpose of domains is for managed service providers can build one Symantec Endpoint Protection Manager infrastructure that services multiple customers.

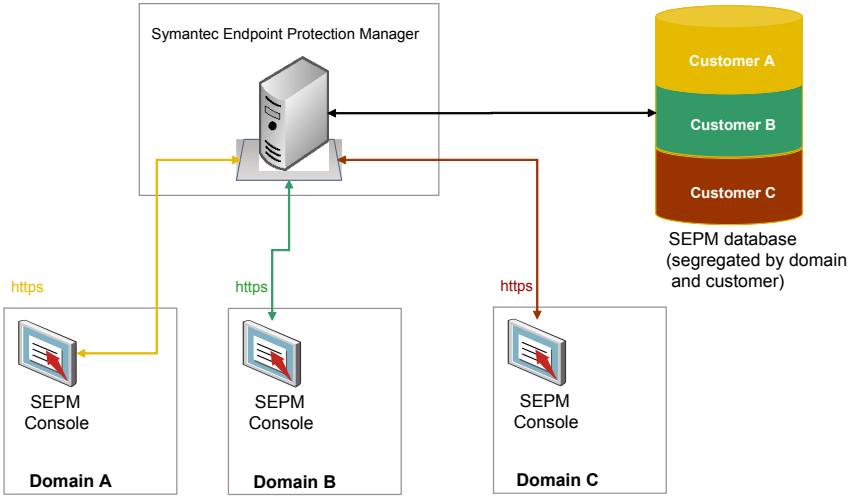
Note: The domains in Symantec Endpoint Protection Manager are not equivalent to Windows domains or other network domains.

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 14-1 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 administrators, groups, clients, computers, and policies to this domain.

You can copy policies 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.

You can also move clients from one domain to another. To move clients between domains, the administrator of the old domain must delete the client from the client group. You then replace the Communication Settings file on the client with one from the new domain.

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 308.

See “Managing administrator accounts” on page 279.

See “Switching to the current domain” on page 309.

See “Restoring client-server communication settings by using the SylinkDrop tool” on page 772.

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 307.

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 307.

See “Adding a domain” on page 308.

Section 4

Managing protection with security policies

Chapter 15

Using policies to manage security

This chapter includes the following topics:

Updating client policies

You can update the policies on the Symantec Endpoint Protection client computer if you do not think you have the latest. 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 168.

You can only manually update the policy on the client computer. If policy settings prevent you from opening the user interface or the notification area icon, you may not be able to manually update the policy.

See "Preventing and allowing users to change the client's user interface" on page 257.

No command exists in Symantec Endpoint Protection Manager to manually prompt the client to update policies. The client checks in for policy updates based on its update method of pull mode or push mode.

See "Updating policies and content on the client using push mode or pull mode" on page 165.

To update the client policy on the client from the Windows taskbar

1. In the Windows taskbar, in the notification area, right-click the Symantec Endpoint Protection icon.
2. Click **Update Policy**.

To update the client policy from the client user interface

1. On the client computer, click **Help > Troubleshooting**.
2. In the **Troubleshooting** dialog box, in the left column, click **Management**.
3. On the **Management** panel, under **Policy Profile**, click one of the following:
   - Click **Update** to update the policy directly from the management console.
   - Click **Import** to import the policy with one that was exported from the management console. Follow the prompt to select the policy file to import.

See "Performing the tasks that are common to all policies" on page 313.

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 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 316. See "About shared and non-shared policies" on page 324. See "Adding a policy" on page 318.
Lock and unlock policy settings	You can allow or prevent client users from configuring some policy settings and client user interface settings. See "Preventing users from disabling protection on client computers" on page 327.
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 318.
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 or location" on page 321.
Test a policy	Symantec recommends that you always test a new policy before you use it in a production environment.
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 "Updating policies and content on the client using push mode or pull mode" on page 165.
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 322.

Table 15-1 Tasks common to all policies *(continued)*

Task	Description
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 320. See "Copying and pasting a policy on the Policies page" on page 319.
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 324. 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 325.
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 Endpoint Protection policies" on page 323.
Withdraw a policy	If you delete a policy, Symantec Endpoint Protection Manager 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 "Unassigning a policy from a group or location" on page 326.
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 "Using the policy serial number to check client-server communication" on page 168. See "Updating client policies" on page 313.

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 313.

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. **Note:** Download Insight and SONAR technology are available only on Windows clients. See "Managing scans on client computers" on page 415.
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 336.

Table 15-2 Security policy types *(continued)*

Policy type	Description
Intrusion Prevention policy	The **Intrusion Prevention policy** automatically detects and blocks network attacks and attacks on browsers as well as protects applications from vulnerabilities. See "Managing intrusion prevention" on page 377.
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 "How to update content and definitions on the clients" on page 178.
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 control" on page 503. Application Control policy can be applied only to Windows clients. The Device Control policy applies to Windows and Mac computers.
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 "Setting up Host Integrity" on page 606.
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 in Symantec Endpoint Protection" on page 544.
Memory Exploit Mitigation	The **Memory Exploit Mitigation policy** stops vulnerability attacks on software using mitigation techniques such as DLL hijacking, heapspray mitigation, and Java exploit prevention. See "Hardening Windows clients against memory tampering attacks with a Memory Exploit Mitigation policy" on page 393.

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 or location" on page 321.

See "Performing the tasks that are common to all policies" on page 313.

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 "Assigning a policy to a group or location" on page 321.

To edit a policy on 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 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 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.

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.

   To redisplay the **Do not show this message again** check box, click **Admin** > **Administrators**, select your administrator account, and click **Reset Copy Policy Reminder**.
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**.

See "Copying and pasting a policy on the Clients page" on page 320.

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 313.

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**.

Assigning a policy to a group or location

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. Typically, you create separate groups for the clients that run different platforms. If you put the clients that run different platforms into the same group, each client platform ignores any settings that do not apply to it.

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. Newly created child groups inherit from **My Company** by default. New groups always inherit from their immediate parent group. If you create a hierarchy of child groups, each one inherits from its immediate parent, not from the top-level parent.
- 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.

The icons display the following information:

Table 15-3 Policy icons

Icon	Description
	A group without a policy that is assigned to it.
	A group with a policy assigned to it. The text is bold.
	A location without a policy that is assigned to it.
	A location with a policy assigned to it. The text is bold.
	A location that inherits from a parent group and has no policy that is assigned to it.
	A location that inherits from a parent group and has a policy that is assigned to it

To assign a policy to a group or location

1. In the console, click **Policies** > *policy type*.
2. On the **Policies** page, select a policy, and then click **Assign the policy**.
3. In the **Assign policy** dialog box, select the groups or locations, and then click **Assign**.
4. Click **OK** to confirm.

See "Unassigning a policy from a group or location" on page 326.

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 313.

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 Endpoint Protection 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 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.

See "Performing the tasks that are common to all policies" on page 313.

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**.

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 318.
- Copy an existing policy to base the new policy on.
  See "Copying and pasting a policy on the Policies page" on page 319.
  See "Copying and pasting a policy on the Clients page" on page 320.
- Import a policy that was previously exported from another site.
  See "Exporting and importing individual Endpoint Protection policies" on page 323.

See "Performing the tasks that are common to all policies" on page 313.

See "Converting a shared policy to a non-shared policy" on page 325.

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 324.

See "Copying and pasting a policy on the Policies page" on page 319.

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 313.

Unassigning a policy from a group or location

You may want to unassign a policy from a group or a location if you want to delete the policy permanently or save the policy to use for a later time.

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 322.

See "Assigning a policy to a group or location" on page 321.

To unassign 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 unassign 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 313.

Preventing users from disabling protection on client computers

As the Symantec Endpoint Protection Manager administrator, you prevent users from disabling protection on the client computer by setting the user control level or by locking the policy options. For example, the firewall policy uses a control level, whereas Virus and Spyware Protection policy uses a lock.

Symantec recommends that you prevent users from disabling protection at all times.

- What are the user control levels?

- Changing the user control level
- Locking and unlocking policy settings
- Preventing users from disabling specific protection technologies
- Updating the client policy from Symantec Endpoint Protection Manager

What are the user control levels?

You use the user control levels to give the client user control of specific features. The user control level also determines whether the client user interface can be completely invisible, display a partial set of features, or display in full.

Table 15-4 User control levels

User control level	Description
Server control	Gives the users the least control over the client. With server control, the user can make changes to unlocked settings, but they are overwritten at the next heartbeat.
Client control	Gives the users the most control over the client. Client control allows users to configure the settings. 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. Client control is useful for employees who work in a remote location or a home location. **Note:** The user must be in a Windows administrators group to change any of the settings in **Client control** mode or **Mixed control** mode.
Mixed control	Gives the user a mixture of control over the client. You determine which options you let users configure by setting the option to **Server control** or to **Client control**. For those items that are under client control, the user retains control over the setting. For those items that are under server control, you retain control over the setting.

For the Windows client, you can configure all the options. For the Mac client, only the notification area icon and some IPS options are available in server control and client control.

Clients that run in **Client control** or **Mixed control** switch to **Server control** when the server applies a Quarantine policy.

See "Preventing and allowing users to change the client's user interface" on page 257.

Changing the user control level

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.

To change the user control level

1. In the console, click **Clients**.
2. Under **View Clients**, select the group, and click the **Policies** tab.
3. Under **Location-specific Policies and Settings**, under the location you want to modify, expand **Location-specific Settings**.
4. Next to **Client User Interface Control Settings**, click **Tasks > Edit Settings**.
5. 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**.
6. Click **OK**.

See "Configuring firewall settings for mixed control" on page 371.

Locking and unlocking policy settings

You can lock and unlock some policy settings. Users cannot change locked settings. A padlock icon appears next to a lockable setting. You can lock and unlock Virus and Spyware Protection settings, Tamper Protection settings, Submissions settings, and intrusion prevention settings.

Preventing users from disabling specific protection technologies

If you set the client to **Mixed control** or **Server control** but do not lock the options, then the user can change the settings. These changes remain in place until the next heartbeat with Symantec Endpoint Protection Manager. Locking the policy options in the various policies ensures that the user cannot make any changes to the settings, even in **Client control**.

Note: Windows users who are not the Administrators group cannot change settings in the Symantec Endpoint Protection client user interface, regardless of the **Location-specific Settings** configuration. Windows 10 Administrators can still disable the product through the notification area icon even after you set these options. However, they cannot disable the individual protection technologies through the client user interface.

Note: If you do not want to change policies for all groups, disable policy inheritance on the group on which you want to make changes. If you edit a shared policy, the edited policy applies to every group to which the shared policy applies, even with policy inheritance disabled.

To prevent users from disabling the firewall or Application and Device Control

1. In the console, click **Clients**.
2. Click the client group that you want to restrict, and then click the **Policies** tab.
3. Expand **Location-specific Settings**.
4. Next to **Client User Interface Control Settings,** click **Tasks > Edit Settings**.
5. Click **Server control** or **Mixed control**, and then click **Customize**.
6. On the **Client User Interface Settings** dialog box (server control) or pane (mixed control), uncheck **Allow the following users to enable and disable the firewall** and **Allow user to enable and disable the application device control**.
7. Click **OK**, and then click **OK** again.

To prevent users from disabling intrusion prevention

1. In the console, click **Clients**.
2. Click the client group that you want to restrict, and then click the policy **Policies** tab.
3. Expand **Location-specific Policies**.
4. Next to **Intrusion Prevention policy**, click **Tasks > Edit Policy**.
5. Click **Intrusion Prevention**, and then click the locks next to **Enable Network Intrusion Prevention** and **Enable Browser Intrusion Prevention** to lock these features.
6. Click **OK**.

To prevent users from disabling Virus and Spyware Protection

1. In the console, click **Clients**.
2. Click the client group that you want to restrict, and then click the **Policies** tab.
3. Expand **Location-specific Policies**.
4. Next to **Virus and Spyware Protection policy**, click **Tasks > Edit Policy**.
5. Under **Windows Settings**, lock the following features:
   - Click **Auto-Protect**, and then click the lock next to **Enable Auto-Protect**.
   - Click **Download Protection**, and then click the lock next to **Enable Download Insight to detect potential risks downloaded files based on file reputation**.
   - Click **SONAR**, and then click the lock next to **Enable SONAR**.
   - Click **Early Launch Anti-Malware Driver**, and then click the lock next to **Enable Symantec early launch anti-malware**.
   - Click **Microsoft Outlook Auto-Protect**, and then click the lock next to **Enable Microsoft Outlook Auto-Protect**.

- For versions earlier than 14.2 RU1, click **Internet Email Auto-Protect**, and then click the lock next to **Enable Internet Email Auto-Protect**.
- For versions earlier than 14.2 RU1, click **Lotus Notes Auto-Protect**, and then click the lock next to **Enable Lotus Notes Auto-Protect**.
- Click **Global Scan Options**, and then click the locks next to **Enable Insight for** and **Enable Bloodhound heuristic virus detection**.

6 Click **OK**.

To prevent users from disabling Memory Exploit Mitigation (starting in 14.0.1)

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

2 Click the client group that you want to restrict, and then click the policy **Policies** tab.

3 Expand **Location-specific Settings**.

4 Next to **Memory Exploit Mitigation**, click **Tasks > Edit Policy**.

5 Click **Memory Exploit Mitigation**, and then click the lock next to **Enable Memory Exploit Mitigation**.

6 Click **OK**.

Updating the client policy from Symantec Endpoint Protection Manager

After you make these changes, the clients in the group receive the updated policies depending on the group's communication settings. If the group is in push mode, Symantec Endpoint Protection Manager prompts the client to check in with a few seconds. If the group is in pull mode, the client checks in on the next scheduled heartbeat.

If you want them to have it sooner than the next heartbeat, you can prompt the client to check in and update its policy. You can also update the policy from the Symantec Endpoint Protection client.

See "Updating client policies" on page 313.

Once the client updates the policy, **Disable Symantec Endpoint Protection** is grayed out when you right-click the Symantec Endpoint Protection notification area icon.

Monitoring the applications and services that run on client computers

The Windows 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
- Host Integrity policies
- Network application monitoring
- File fingerprint lists

Note: The Mac and Linux clients do not monitor the applications and the services that run on those computers.

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

Table 15-5 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 "Collecting information about the applications that the client computers run" on page 333.
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 334. 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.

Collecting 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 and Linux clients do not monitor the applications and the services that run on those 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 671.

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 331.

See "Performing the tasks that are common to all policies" on page 313.

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 352.

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 331.

See "Performing the tasks that are common to all policies" on page 313.

Chapter 16

Managing firewall protection

This chapter includes the following topics:

Managing firewall protection

The firewall allows the incoming network traffic and outgoing network traffic that you specify in the firewall policy. The Symantec Endpoint Protection firewall policy contains rules and protection settings, most of which you can enable or disable and configure.

Table 16-1 Optional tasks to 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 338. See "About the Symantec Endpoint Protection firewall" on page 338.
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 340.
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 "Adding a new firewall rule" on page 344. See "Customizing firewall rules" on page 362.
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 "Enabling communications for network services instead of adding a rule" on page 372. See "Automatically blocking connections to an attacking computer" on page 373. See "Preventing outside stealth attacks on computers" on page 375. See "Disabling the Windows Firewall" on page 376. See "Blocking a remote computer by configuring peer-to-peer authentication" on page 615.
Monitor firewall protection	Regularly monitor the firewall protection status on your computers. See "Monitoring endpoint protection" on page 625.

See "Running commands on client computers from the console" on page 253.

See "Configuring firewall settings for mixed control" on page 371.

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 unit 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 include the following information about the data:

- The originating computer
- The intended recipient or 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 338.

See “Managing firewall protection” on page 336.

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 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.

As of version 14.2, the Mac client offers a firewall for the managed client only. The user can only enable or disable the firewall if the administrator has allowed client control. Since it operates on a different network layer than the Mac's operating system firewall, they can both be enabled and run in parallel.

See “About firewall settings for the Mac client” on page 339.

See “Managing firewall protection” on page 336.

See “How a firewall works” on page 338.

See “How the firewall uses stateful inspection” on page 350.

See “The types of security policies” on page 316.

About firewall settings for the Mac client

The firewall settings that are included in the Symantec Endpoint Protection client for Mac are as follows:

- Firewall smart rules
- Custom firewall rules

These settings are only configurable by the Symantec Endpoint Protection Manager administrator. The firewall is only available to managed clients.

Table 16-2 Firewall settings

Setting type	Description
Firewall smart rules	Firewall smart rules provide protection to prevent common types of attack. They also allow traffic on specific protocols when the Mac makes the initial request on that protocol. Protection settings include: ■ Portscan detection ■ Denial of service detection ■ Anti-MAC spoofing ■ Automatically block an attacker's IP address Traffic protocols include: ■ Smart DHCP ■ Smart DNS The Symantec Endpoint Protection firewall for Mac does not integrate with the operating system's built-in firewall. Instead, it runs in parallel. The operating system firewall inspects at the Application layer, while the Symantec Endpoint Protection firewall inspects at lower levels (Network and Transport). The Symantec Endpoint Protection firewall for Mac does not offer peer-to-peer blocking rules, though you could create these in part through custom firewall rules.
Custom firewall rules	Custom firewall rules allow the administrator to create the rules that involve various attributes of the network traffic.

See "Managing firewall protection" on page 336.

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.

Note: Changing the name of the default Firewall policy may result in an upgrade not updating the policy. The same applies to the default rules within the default Firewall policy.

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.

Table 16-3 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 16-3 How to create a firewall policy

Task	Description
Add new 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 that are enabled by default. See "Adding a new firewall rule" on page 344.
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 355.
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 "Enabling communications for network services instead of adding a rule" on page 372. 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 373.

Table 16-3 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. You can enable the settings that prevent outside attacks from detecting information about your clients. See "Preventing outside stealth attacks on computers" on page 375. 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 376.
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. This option is disabled by default. See "Blocking a remote computer by configuring peer-to-peer authentication" on page 615.

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.

See "Managing firewall protection" on page 336.

See "Best practices for Firewall policy settings for remote clients" on page 274.

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 16-4 describes what you need to know to manage firewall rules.

Table 16-4 Managing firewall rules

Task	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 345. ■ 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 347. ■ The implications of inheriting rules from a parent group and how inherited rules are processed See "About inherited firewall rules" on page 348. ■ That the client uses stateful inspection, which keeps track of the state of the network connections See "How the firewall uses stateful inspection" on page 350. ■ 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 351. See "About firewall rule host triggers" on page 355. See "About firewall rule network services triggers" on page 359. See "About firewall rule network adapter triggers" on page 360.

Table 16-4 Managing firewall rules *(continued)*

Task	Description
Add a new firewall rule	You can perform the following tasks to manage firewall rules: ■ 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 344. ■ Customize a rule by changing any of the firewall rule criteria ■ Export and import firewall rules from another firewall policy See "Importing and exporting firewall rules" on page 362. ■ 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.
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 362.

See "Managing firewall protection" on page 336.

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 345.
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 firewall rule using a wizard" on page 345.

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, under **Windows Settings** or **Mac Settings**, click **Rules**.
3. On the **Rules** tab, under the **Rules** list, click **Add Blank Rule**.
4. Optionally, you can change the firewall rule criteria as needed.
5. If you are done with the configuration of the rule, click **OK**.

To add a firewall rule using a wizard

1. In the console, open a Firewall policy.
2. On the **Firewall Policy** page, under **Windows Settings** or **Mac Settings**, click **Rules**.

   On the **Rules** tab, under the **Rules** list, click **Add Rule**.
3. Fill out the options on each screen, and then click **Next**.
4. Click **Finish**.

   Optionally, you can change the firewall rule criteria as needed.

See "Customizing firewall rules" on page 362.

See "How the firewall uses stateful inspection" on page 350.

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.

All rules on the Mac client are server rules. Mac users do not have the option of creating client rules for the Mac client.

Table 16-5 describes the relationship between the client's user control level and the user's interaction with the firewall rules.

Table 16-5 User control level and rule status

User control level	User interaction
Server control	The Windows client receives server rules but the user cannot view them. The user cannot create client rules. The Mac client does not allow the user to enable or disable the firewall.

Table 16-5 User control level and rule status *(continued)*

User control level	User interaction
Mixed control	The Windows client receives server rules. The user can create client rules, which are merged with server rules and client security settings. The Mac client allows or disallows the user to enable or disable the firewall. It depends on whether the granular setting is set to server control or client control.
Client control	The client does not receive server rules. The user can create client rules. The Symantec Endpoint Protection Manager administrator cannot view client rules. The Mac client allows the user to enable or disable the firewall.

See "Preventing users from disabling protection on client computers" on page 327.

Table 16-6 lists the order that the firewall processes server rules, client rules, and client settings.

Table 16-6 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 343.

See "Changing the order of firewall rules" on page 350.

See "Preventing users from disabling protection on client computers" on page 327.

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 Windows client is set to mixed control. The firewall processes both server rules and client rules.

Table 16-7 shows the order in which the firewall processes the rules, firewall settings, and intrusion prevention settings.

Table 16-7 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 350.

See “Managing firewall rules” on page 343.

See “How a firewall works” on page 338.

See “How intrusion prevention works” on page 380.

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 italics (version 14.x) or purple (version 12.1.x). Above the blue line, the inherited rules are added above the rules that you created as Symantec Endpoint Protection Manager administrator. 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.

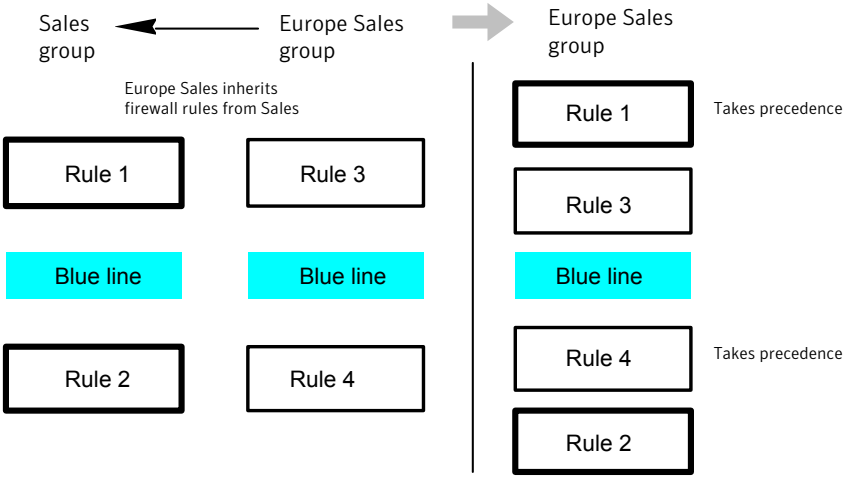
If you want to remove the inherited rules, you remove the inheritance rather than delete them. You have to remove all the inherited rules rather than the selected rules.

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 16-1 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 16-1 An example of how firewall rules inherit from each other



See "Managing firewall rules" on page 343.

See "Adding inherited firewall rules from a parent group" on page 349.

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, under **Windows Settings** or **Mac Settings**, 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 318.

See "About inherited firewall rules" on page 348.

See "Managing firewall rules" on page 343.

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.

If the Symantec Endpoint Protection client uses location switching, when you change the firewall rule order, the change affects the order for the current location only.

Note: For better protection, place the most restrictive rules first and the least restrictive rules last.

See "About the firewall rule, firewall setting, and intrusion prevention processing order" on page 347.

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 "Editing a policy" on page 318.

See "Managing firewall rules" on page 343.

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.

The state table that maintains the connection information may be periodically cleared. For example, it is cleared when a Firewall policy update is processed or if Symantec Endpoint Protection services are restarted.

See "How a firewall works" on page 338.

See "Managing firewall rules" on page 343.

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 352.

See "Notifying the users that access to an application is blocked" on page 355.

See “Managing firewall rules” on page 343.

See “Blocking networked applications that might be under attack” on page 353.

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 352.
- 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 353.

To define information about applications manually

1. In the console, open a Firewall policy.
2. On the **Firewall Policies** page, under **Windows Settings**, click **Rules**.
3. On the **Rules** tab, in the **Rules** list, right-click the **Application** field for the rule you want to change, 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:
   - File name, which can include the file path
   - File description
     This field is used for display purposes only. It does not function as a matching condition.
   - File size, in bytes
   - Date that the application was last changed
   - File fingerprint

   Note: Network Application Monitoring must be enabled to define a firewall rule by file size, date last modified, or file fingerprint. If Network Application Monitoring is disabled, rule processing ignores all fields except for **File Name**.
6. Click **OK** to add the application conditions.
7. Click **OK** to save the application list.

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 343.

See "Editing a policy" on page 318.

See "About firewall rule application triggers" on page 351.

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 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 343.

See "Notifying the users that access to an application is blocked" on page 355.

See “About firewall rule application triggers” on page 351.

See “Searching for information about the applications that the computers run” on page 334.

See “Collecting information about the applications that the client computers run” on page 333.

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 **Display notification on the computer when the client blocks an application** and optionally add a custom message.
4. Click **OK**.

See “Managing firewall rules” on page 343.

See “Configuring client notifications for intrusion prevention and Memory Exploit Mitigation” on page 386.

See “Setting up administrator notifications” on page 671.

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 are 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 16-2 illustrates the source relationship and destination relationship with respect to the direction of traffic.

Figure 16-2 The relationship between source and destination hosts

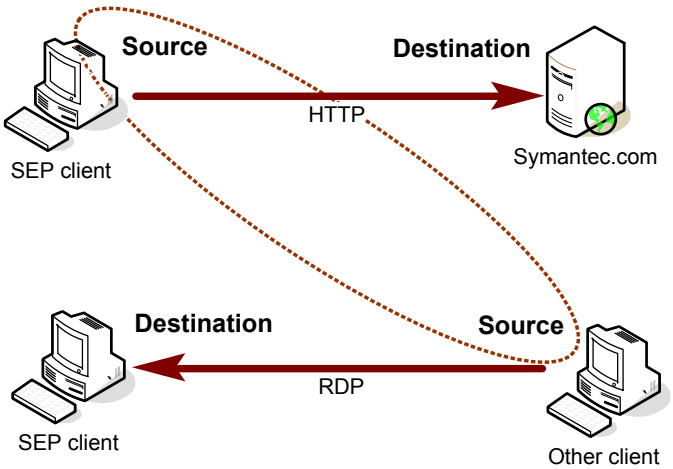
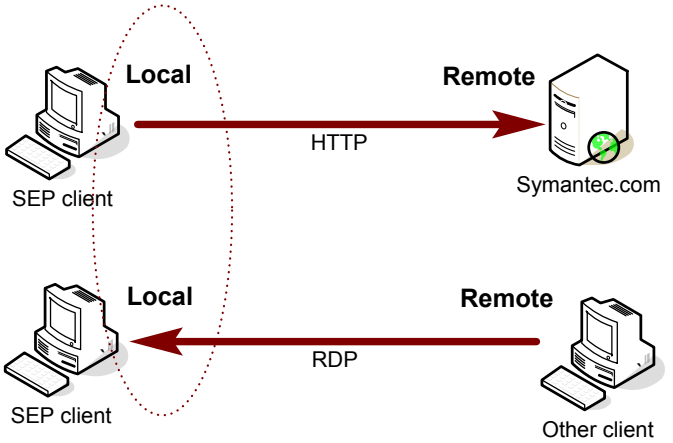


Figure 16-3 illustrates the local host and remote host relationship with respect to the direction of traffic.

Figure 16-3 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 357.

See "Blocking traffic to or from a specific server" on page 365.

See "Managing firewall rules" on page 343.

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 355.

Defining DNS queries based on location

You can define how frequently you want a specific location to perform a DNS query on the . 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 343.

See "About firewall rule host triggers" on page 355.

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 359.

See "Permitting clients to browse for files and printers in the network" on page 367.

See "Managing firewall rules" on page 343.

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. If you install the client on the computers that run Windows 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 343.

See "About firewall rule network services triggers" on page 359.

See "Controlling whether networked computers can share messages, files, and printing" on page 367.

See "Permitting clients to browse for files and printers in the network" on page 367.

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.

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 343.

See "Adding a custom network adapter to the network adapter list" on page 361.

See "Controlling the traffic that passes through a network adapter" on page 370.

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 343.

See "About firewall rule network adapter triggers" on page 360.

See “Controlling the traffic that passes through a network adapter” on page 370.

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, under **Windows Settings** or **Mac Settings**, 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, under **Windows Settings** or **Mac Settings**, 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 “Adding a new firewall rule” on page 344.

See “Customizing firewall rules” on page 362.

See “About the firewall rule, firewall setting, and intrusion prevention processing order” on page 347.

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.

Note: The Mac client firewall monitors packets but does not log them.

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 351.
- 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 355.
- 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 359.
- 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 360.

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.

To customize firewall rules

1. In the console, open a Firewall policy.
2. On the **Firewall Policy** page, under **Windows Settings** or **Mac Settings**, 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 352.
7. In the **Host** field, specify a host trigger.

   See "Blocking traffic to or from a specific server" on page 365.
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 366.
9. In the **Service** field, specify a network service trigger.

   See "Controlling whether networked computers can share messages, files, and printing" on page 367.
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 369.
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 370.

13 In the **Time** column, specify the time periods in which this rule is active.

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 “Adding a new firewall rule” on page 344.

See “Managing firewall rules” on page 343.

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 add to the rule.

6 Add additional hosts, if necessary.

7 Click **OK** to return to the **Rules** list.

See "Adding a new firewall rule" on page 344.

See "Customizing firewall rules" on page 362.

See "Adding host groups" on page 357.

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, under **Windows Settings** or **Mac Settings**, click **Rules**.

3 On the **Rules** tab, in the **Firewall Rules** table, find the rule that you want to edit.

4 Double-click in the **Host** column for 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 one of the following:

- Windows: **Local Subnet**
- Mac: **Subnet**

7 Click **OK**, and then click **OK** again to close out of the **Host List** dialog box.

See "Customizing firewall rules" on page 362.

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, under **Windows Settings** or **Mac Settings**, click **Rules**.
3. On the **Rules** tab, in the **Rules** list, select the rule you want to edit, right-click the **Service** field, and then click **Edit**.
4. In the **Service List** dialog box, check the 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 "Adding a new firewall rule" on page 344.

See "Customizing firewall rules" on page 362.

See "About firewall rule network services triggers" on page 359.

See "Adding network services to the default network services list" on page 359.

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 Windows client can enable these settings automatically by configuring them in Network and Host Exploit Mitigation. Users on the Mac client can only enable or disable the firewall.
Mixed control	A server firewall rule that specifies this type of traffic can override these settings on Windows. All firewall rules are server firewall rules on a Mac.
Server control	These settings are not available on the client.

To permit Windows clients to browse for files and printers in the network

1. In the console, open a Firewall policy.
2. On the **Firewall Policy** page, under **Windows Settings**, 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**.

To permit Mac clients to browse for files and printers in the network

1 In the console, open a Firewall policy.

2 On the **Firewall Policy** page, under **Mac Settings**, 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 To enable other computers to browse files on the client, in the **Local Port** drop-down list, type **139** and **445**.

Outgoing requests to browse the network from the Mac are enabled by default.

7 Click **OK**.

8 In the **Service List** dialog box, make sure that the new service is enabled, and then click **OK**.

9 On the **Rules** tab, make sure the **Action** field is set to **Allow**.

10 If you are done with the configuration of the policy, click **OK**.

Printer discovery on Macs is through the Bonjour service, which is open by default. You do not need to configure a custom rule for the Bonjour service.

See "Adding a new firewall rule" on page 344.

See "Customizing firewall rules" on page 362.

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, under **Windows Settings** or **Mac Settings**, click **Rules**.

3 On the **Rules** tab, select a rule, right-click the **Log** 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	For Windows rules, check both **Write to Traffic Log** and **Write to Packet Log**. For Mac rules, check **Write to Traffic 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 "Adding a new firewall rule" on page 344.

See "Customizing firewall rules" on page 362.

See "Setting up administrator notifications" on page 671.

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, under **Windows Settings**, 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 "Adding a new firewall rule" on page 344.

See "Customizing firewall rules" on page 362.

See "About firewall rule network adapter triggers" on page 360.

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.

For the Mac firewall, the user cannot create firewall rules or change settings regardless of the client user interface settings. The options do not ever appear in the client user interface.

Server control	For Windows, the user cannot create any firewall rules or enable firewall settings. For Mac, the user cannot enable or disable the firewall.
Client control	For Windows, the user can create firewall rules and enable all firewall settings. For Mac, the user can enable and disable the firewall.
Mixed control	For Windows, the user can create firewall rules. You decide which firewall settings the user can enable. For Mac, you decide whether the user can enable or disable the firewall.

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 336.

See "Enabling communications for network services instead of adding a rule" on page 372.

Enabling communications for network services instead of adding a rule

You can enable the options that automatically allow 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 enable communications for network services instead of adding a rule

1. In the console, open a Firewall policy.
2. On the **Firewall Policy** page, under **Windows Settings** or **Mac Settings**, 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 340.

See "Editing a policy" on page 318.

See "Preventing users from disabling protection on client computers" on page 327.

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 one of the following options:
   - Under **Windows Settings**: **Protection and Stealth**
   - Under **Mac Settings**: **Protection**
3. Under **Protection Settings**, 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 340.

See "Configuring firewall settings for mixed control" on page 371.

See "Editing a policy" on page 318.

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 this setting is enabled, Symantec Endpoint Protection allows the following incoming and outgoing traffic if a request was made to that specific host: ■ Address resolution protocol (ARP) (IPv4) ■ Neighbor Discovery Protocol (NDP) (IPv6) All other unexpected 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 one of the following:
   - Under **Windows Settings**: **Protection and Stealth**
   - Under **Mac Settings**: **Protection**
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 340.

See "Preventing users from disabling protection on client computers" on page 327.

See "Editing a policy" on page 318.

Preventing outside stealth attacks on computers

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.

Note: These stealth settings are not available for the Mac firewall.

To prevent outside stealth attacks on computers

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.
4. Click **OK**.
5. If you are prompted, assign the policy to a location.

See "Creating a firewall policy" on page 340.

See "Preventing users from disabling protection on client computers" on page 327.

See "Editing a policy" on page 318.

Disabling the Windows Firewall

You can specify the conditions in which Symantec Endpoint Protection disables Windows Firewall. Symantec Endpoint Protection restores the Windows Firewall settings to the state it was in before Symantec Endpoint Protection was installed when the following occurs:

- Symantec Endpoint Protection is uninstalled.
- The Symantec Endpoint Protection firewall is disabled.

Note: Symantec Endpoint Protection does not modify any existing Windows Firewall policy rules or exclusions.

Typically, a Windows user receives a notification when their computer restarts if Windows Firewall is disabled. Symantec Endpoint Protection disables this notification by default so that it does not alarm your users when Windows Firewall is disabled. However, 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 Windows Firewall disabled.

   The default setting is **Disable Once Only**.

   Click **Help** for more information on the options.
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 Windows Firewall is disabled.
7. Click **OK.**

See "Creating a firewall policy" on page 340.

See "The types of security policies" on page 316.

Chapter 17

Managing intrusion prevention and OS hardening

This chapter includes the following topics:

Managing intrusion prevention

The default intrusion prevention settings protect client computers against a wide variety of threats. You can change the default settings for your network.

If you run Symantec Endpoint Protection on servers, intrusion prevention might affect server resources or response time. For more information, see:

Best practices for Endpoint Protection on Windows Servers

Note: The Linux client does not support intrusion prevention.

Table 17-1 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 380. See "About Symantec IPS signatures" on page 381.
Enable intrusion prevention	To keep your client computers secure, you should keep intrusion prevention enabled: ■ Network intrusion prevention ■ Browser intrusion prevention (Windows computers only) You can also configure browser intrusion prevention to only log detections, but not block them. You should use this configuration on a temporary basis as it lowers the client's security profile. For example, you would configure log-only mode only while you troubleshoot blocked traffic on the client. After you review the attack log to identify and exclude the signatures that block traffic, you disable log-only mode. See "Enabling network intrusion prevention or browser intrusion prevention" on page 383. See "Creating exceptions for IPS signatures" on page 384. You can also enable both types of intrusion prevention, as well as the firewall, when you run the **Enable Network Threat Protection** command on a group or client. See "Running commands on client computers from the console" on page 253.

Table 17-1 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. ■ Use audit signatures to monitor certain types of traffic (Windows only) Audit signatures have a default action of **Not log** for certain traffic types, such as traffic from instant message applications. You can create an exception to log the traffic so that you can view the logs and monitor this traffic in your network. You can then use the exception to block the traffic, create a firewall rule to block the traffic, or leave the traffic alone. You can also create an application rule for the traffic. See "Creating exceptions for IPS signatures" on page 384. You can use application control to prevent users from running peer-to-peer applications on their computers. See "Adding custom rules to Application Control" on page 507. 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 340.

Table 17-1 Managing intrusion prevention *(continued)*

Task	Description
Create exceptions to ignore browser signatures on client computers (Windows only)	You can create exceptions to exclude browser signatures from browser intrusion prevention on Windows computers. 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 384.
Exclude specific computers from network intrusion prevention scans	You might want to exclude certain computers from network 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 385.
Configure intrusion prevention notifications	By default, messages appear on client computers for intrusion attempts. You can customize the message. See "Configuring client notifications for intrusion prevention and Memory Exploit Mitigation" on page 386.
Create custom intrusion prevention signatures (Windows only)	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 websites. See "Managing custom intrusion prevention signatures" on page 387. You must have the firewall installed and enabled to use custom IPS signatures. See "Choosing which security features to install on the client" on page 121.
Monitor intrusion prevention	Regularly check that intrusion prevention is enabled on the client computers in your network. See "Monitoring endpoint protection" on page 625.

How intrusion prevention works

Intrusion prevention and the firewall are part of Network Threat Protection. As of version 14, Network Threat Protection and Memory Exploit Mitigation are part of Network and Host Exploit Mitigation.

Intrusion prevention automatically detects and blocks network attacks. On Windows computers, intrusion prevention also detects and blocks browser attacks on supported 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.

Table 17-2 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 in Symantec Endpoint Protection Manager. You cannot create custom signatures on the client directly; however, you can import custom signatures on the client. Custom signatures are supported on Windows computers only. See "About Symantec IPS signatures" on page 381.
Browser intrusion prevention (Windows only)	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 turn it back on. 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. For the latest information about the browsers that browser intrusion prevention protects, see: Supported browser versions for browser intrusion prevention.

See "Managing intrusion prevention" on page 377.

About Symantec IPS signatures

Symantec intrusion prevention signatures are installed on the client by default.

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, which are downloaded to the client as part of LiveUpdate content. For Mac computers, there are some additional network intrusion prevention signatures that are built into the software.

On Windows computers, LiveUpdate content also includes signatures for 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 (Windows only)	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. You can configure browser intrusion prevention to log the browser detections but not block them. This action helps you identify those browser signatures that you may need to exclude. After you create the signature exclusions, you disable log-only mode.

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 website page:

Attack Signatures

For information about the built-in IPS signatures for Mac clients, see the following article:

Built-in signatures for Symantec Endpoint Protection IPS for Mac

See “Creating exceptions for IPS signatures” on page 384.

See “Managing intrusion prevention” on page 377.

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.

Note: You must have the firewall installed and enabled to use custom IPS signatures.

See “Choosing which security features to install on the client” on page 121.

Custom signatures are supported on Windows computers only.

See “Managing custom intrusion prevention signatures” on page 387.

Enabling network intrusion prevention or browser intrusion prevention

Intrusion prevention is enabled by default. Typically, you should not disable either type of intrusion prevention.

You can enable a log-only mode for browser intrusion prevention to record what traffic it blocks without affecting the client user. You can then use the **Network and Host Exploit Mitigation** attack logs in Symantec Endpoint Protection Manager to create exceptions in the **Intrusion Prevention** policy to ignore specific browser signatures. You would then disable log-only mode.

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 enable network intrusion prevention or browser intrusion prevention

1. In the console, open an Intrusion Prevention policy.
2. On the policy page, click **Intrusion Prevention**.
3. Make sure the following options are checked:
   - **Enable Network Intrusion Prevention**
     You can also exclude particular computers from network intrusion prevention.
     See “Setting up a list of excluded computers” on page 385.
   - **Enable Browser Intrusion Prevention for Windows**
4. Click **OK**.

See “Creating exceptions for IPS signatures” on page 384.

See “Managing intrusion prevention” on page 377.

See “Configuring firewall settings for mixed control” on page 371.

Creating exceptions for IPS signatures

You use exceptions to change the behavior of Symantec IPS signatures.

For Windows and Mac computers, 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.

For Windows computers, 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 Log**. You cannot customize the action or the log setting.

See “Managing intrusion prevention” on page 377.

Note: To change the behavior of a custom IPS signature that you create or import, you edit the signature directly. Custom signatures are supported on Windows computers only.

To create an exception for IPS signatures

1. In the console, open an Intrusion Prevention policy.
2. Under **Windows Settings** or **Mac Settings**, click **Exceptions**, and then click **Add**.

   Note: The signatures list populates with the latest LiveUpdate content that the management console downloaded. For Windows computers, the list appears blank if the management server has not yet downloaded the content. For Mac computers, the list always contains at least the built-in signatures, which are installed automatically on your Mac clients.

   ---

3. In the **Add Intrusion Prevention Exceptions** dialog box, do the following actions to filter the signatures:
   - (Windows only) To display only the signatures in a particular category, select an option from the **Show category** drop-down list. If you select **Browser Protection**, the signature action options automatically change to **Allow** and **Do Not Log**.

- (Windows and Mac) 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 signatures the same, click **Select All**.

5 Click **Next**.

6 In the **Signature Action** dialog box, set the following options and then click **OK**.

- Set **Action** to **Block** or **Allow**
- Set **Log** to **Log the traffic** or **Do not log the traffic**.

Note: These options only apply to network signatures. For browser signatures, click **OK**.

If you want to revert the signature's behavior back to the original behavior, select the signature in the **Exceptions** list, and then click **Delete**.

7 Click **OK** to save the policy changes.

See "Managing exceptions in Symantec Endpoint Protection" on page 544.

Setting up a list of excluded computers

Excluded hosts are supported for network intrusion prevention only.

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. Network intrusion prevention and peer-to-peer authentication allow any source traffic from hosts in the excluded hosts list. However, network intrusion prevention and peer-to-peer authentication continue to evaluate any destination traffic to hosts in the list. The list applies to both inbound traffic and outbound traffic, but only to the source of the traffic. The list also applies only to remote IP addresses.

For example, you might 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 policy page, click **Intrusion Prevention**.

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 from network intrusion prevention.

See "Blocking traffic to or from a specific server" on page 365.

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 notifications for intrusion prevention and Memory Exploit Mitigation

By default, notifications appear on client computers when the client detects intrusion protection events and Memory Exploit Mitigation. When these notifications are enabled, they display a standard message. For IPS notifications, you can add customized text to the standard message.

To configure client notifications for intrusion prevention and Memory Exploit Mitigation

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 and Memory Exploit Mitigation notifications**.

7 To enable a sound when the notification appears, click **Use sound when notifying users**.

8 Click **OK**.

9 Click **OK**.

See "Managing intrusion prevention" on page 377.

See "Hardening Windows clients against memory tampering attacks with a Memory Exploit Mitigation policy" on page 393.

See "Setting up administrator notifications" on page 671.

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.

Note: You must have the firewall installed and enabled to use custom IPS signatures. See "Choosing which security features to install on the client" on page 121.

Table 17-3 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 "About custom IPS signatures" on page 382. See "Creating a custom IPS library" on page 388.

Table 17-3 Managing custom intrusion prevention signatures *(continued)*

Task	Description
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 389.
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 392.
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 391.
Copy and paste signatures	You can copy and paste signatures between groups and between libraries.
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 391.
Test custom signatures	You should test the custom intrusion prevention signatures to make sure that they work. See "Testing custom IPS signatures" on page 393.

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 387.

To create a custom IPS library

1. In the console, on the **Policies** page, under **Policies**, click **Intrusion Prevention**.
2. Click the **Custom Intrusion Prevention** tab.
3. Under **Tasks**, click **Add Custom Intrusion Prevention Signatures**.

4 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.

5 To add a new group, on the **Signatures** tab, under the **Signature Groups** list, click **Add**.

6 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**.

7 Add a custom signature.

See "Adding signatures to a custom IPS library" on page 389.

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 387.

To add a custom signature

1 Create a custom IPS library.

See "Creating a custom IPS library" on page 388.

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 392.

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 387.

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**.

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 387.

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**.

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 387.

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**.

Testing custom IPS signatures

After you create custom IPS signatures, you should test them to make sure that they function correctly.

Table 17-4 Testing custom IPS signatures

Step	Description
Step 1: Make sure that clients use the current policy	The next time that the client receives the policy, the client applies the new custom signatures. See "Updating client policies" on page 313.
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 and Host Exploit Mitigation Attack logs. The message you specify in the custom IPS signature appears in the log See "Monitoring endpoint protection" on page 625.

See "Managing custom intrusion prevention signatures" on page 387.

Hardening Windows clients against memory tampering attacks with a Memory Exploit Mitigation policy

- How does Memory Exploit Mitigation protect applications?
- Types of exploit protection
- Memory Exploit Mitigation requirements
- Correcting and preventing false positives
- Finding the logs and reports for Memory Exploit Mitigation events
- Auditing protection for a terminated application
- Disabling Memory Exploit Mitigation
- Reporting false positives to Security Response

How does Memory Exploit Mitigation protect applications?

Starting in 14, Symantec Endpoint Protection includes Memory Exploit Mitigation, which uses multiple mitigation techniques to stop attacks on a vulnerability in the software. For example, when the client user runs an application such as Internet Explorer, an exploit might instead launch a different application that contains malicious code.

To stop an exploit, Memory Exploit Mitigation injects a DLL into a protected application. After Memory Exploit Mitigation detects the exploit attempt, it either blocks the exploit or terminates the application that the exploit threatens. Symantec Endpoint Protection displays a notification to the user on the client computer about the detection, and logs the event in the client's Security log.

For example, the client user might see the following notification:

`Symantec Endpoint Protection: Attack: Structured Exception Handler Overwrite detected. Symantec Endpoint Protection will terminate <application name> application`

Memory Exploit Mitigation continues to block the exploit or terminate the application until the client computer runs a version of the software where the vulnerability is fixed.

Note: In 14 MPx, Memory Exploit Mitigation was called Generic Exploit Mitigation.

Using Generic Exploit Mitigation

Types of exploit protection

Memory Exploit Mitigation uses multiple types of mitigation techniques to handle the exploit, depending on which technique is most appropriate for the type of application. For example, both the StackPvt and RopHeap techniques block the exploits that attack Internet Explorer.

Symantec Endpoint Protection Memory Exploit Mitigation techniques

---

Note: If you have enabled the Microsoft App-V feature on your computers, Memory Exploit Mitigation does not protect the Microsoft Office processes that App-V protects.

Memory Exploit Mitigation requirements

Memory Exploit Mitigation is only available if you have installed intrusion prevention. Memory Exploit Mitigation has its own set of separate signatures that is downloaded along with the intrusion prevention definitions. However, you can enable or disable intrusion prevention and Memory Exploit Mitigation independently.

Note: Starting in 14.0.1, Memory Exploit Mitigation has its own policy. In the 14 MPx releases, it is part of the Intrusion Prevention policy; if you disable the Intrusion Prevention policy on the **Overview** tab, you disable Memory Exploit Mitigation.

See "Enabling network intrusion prevention or browser intrusion prevention" on page 383.

See "Choosing which security features to install on the client" on page 121.

In addition, you must run LiveUpdate at least once for the list of applications to appear in the Memory Exploit Mitigation policy. By default, protection is enabled for all applications that appear in the policy.

See "Checking that Symantec Endpoint Protection Manager has the latest content" on page 190.

Correcting and preventing false positives

Occasionally, Memory Exploit Mitigation may unintentionally terminate an application on the client computer. If you determine that an application's behavior is legitimate and was not exploited, the detection is a false positive. For false positives, you should disable protection until Symantec Security Response changes the Memory Exploit Mitigation behavior.

Table 17-5 displays the steps to handle false positive detections.

Table 17-5 Steps to find and remediate a false positive

Tasks	
Step 1: Find out which applications terminate unexpectedly on the client computers.	You can find out which applications were terminated on the client computer in the following ways: ■ A user on the client computer notifies you that an application does not run. ■ Open the Memory Exploit Mitigation log or report that lists which mitigation technique terminated the applications on the client computer. **Note:** Sometimes the mitigation techniques do not produce logs due to the nature of the exploit. Finding the logs and reports for Memory Exploit Mitigation events

Table 17-5 Steps to find and remediate a false positive *(continued)*

Tasks	
Step 2: Disable protection and audit the techniques that terminate the application.	Disable protection at the most minimal level first so that other processes remain protected. Do not turn off Memory Exploit Mitigation to allow the application to run until you have tried all other methods. After each of the following subtasks, go to Step 3. 1 First, audit the protection for the specific application that the mitigation technique terminated. For example, if Mozilla Firefox was terminated, you would disable either the SEHOP technique or the HeapSpray technique. Sometimes a mitigation technique does not create log events due to the nature of the exploit, so you cannot be sure which mitigation technique terminated the application. In this case, you should disable each technique that protects that application, one at a time, until you find which technique caused the termination. 2 Audit protection for all applications that a single mitigation technique protects. 3 Audit protection for all applications, regardless of the technique. This option is similar to disabling Memory Exploit Mitigation, except that the management server collects the log events for detections. Use this option to check for false positives on legacy 14 MPx clients. Auditing protection for a terminated application
Step 3: Update the policy on the client computer, and rerun the application.	■ If the application runs correctly, the detection for that mitigation technique is a false positive. ■ If the application does not run the way you expect it to, the detection is a true positive. ■ If the application still terminates, audit at a level restrictive level. For example, audit a different mitigation technique or for all applications that the technique protects. See “Updating client policies” on page 313.

Table 17-5 Steps to find and remediate a false positive *(continued)*

Tasks	
Step 4: Report the false positives and reenable protection for the true positives.	For false positive detections: 1 Notify Symantec Security Response that the detection was a false positive. Reporting false positives to Security Response Report a Suspected Erroneous Detection (False Positive) 2 Keep protection disabled for the terminated application by setting each technique's action to **No**. 3 After Security Response resolves the issue, reenable protection by changing the technique's action to **Yes**. For true positive detections: 1 Reenable protection by changing the rule's action for that mitigation technique back to **Yes**. 2 Check whether there is a patched version or a newer release of the infected application that fixes the current vulnerability. After you install the patched application, rerun it on the client computer to see if Memory Exploit Mitigation still terminates the application.

Finding the logs and reports for Memory Exploit Mitigation events

You need to view the logs and run quick reports to find the applications that Memory Exploit Mitigation terminated.

To find the logs and reports for Memory Exploit Mitigation events

- In the console, do one of the following actions:
  - For logs, click **Monitors** > **Logs** > **Network and Host Exploit Mitigation** log type > **Memory Exploit Mitigation** log content > **View Log**.
    Look for the **Memory Exploit Mitigation Blocked Event** event type. The **Event type** column lists the mitigation technique, and the **Action** column lists whether or not the application in the **Application Name** column was blocked. For example, the following log event indicates a Stack Pivot attack:
    ```
    Attack: Return Oriented Programming Changes Stack Pointer
    ```
  - For quick reports, click **Reports** > **Quick Reports** > **Network and Host Exploit Mitigation** report type > **Memory Exploit Mitigation Detections** report > **Create Report**.
    Look for the blocked Memory Exploit Mitigation detections.

Auditing protection for a terminated application

When you test for false positives, change the Memory Exploit Mitigation behavior so that it audits a detection, but lets the application run. However, Memory Exploit Mitigation does not protect the application.

To audit protection for a terminated application

1. In the console, click **Policies** > **Memory Exploit Mitigation** > **Memory Exploit Mitigation**.
2. On the **Mitigation Techniques** tab, next to **Choose a mitigation technique**, select the technique that terminated the application, such as **StackPvt**.
3. Under the **Protected** column, select the terminated application, and then change **Default (Yes)** to **Log Only**.

   Change the action to **No** after you verified that the detection is a true false positive. Both **Log Only** and **No** allow the possible exploit, but also let the application run.

   Some applications have multiple mitigation techniques that block the exploit, so follow this step for each technique individually.
4. (Optional) Do one of the following steps, and then click **OK**:
   - If you are not sure which technique terminated the application, click **Choose a protection action for all applications for this technique**. This option overrides the settings for each technique.
   - If you have a mix of 14.0.1 clients and legacy 14 MPx clients, and you only want to test the 14.0.1 clients, click **Set the protection action for all techniques to log only**.
5. (Optional) To test the application regardless of technique, on the **Application Rules** tab, in the **Protected** column, uncheck the terminated application, and then click **OK**.

   For legacy 14 MPx clients, you can only use this option. After you upgrade to version 14.0.1 clients, reenable protection and do the finer grained tuning. Open the **Computer Status** log to find which clients run which product version.

After steps 3 through 5, run the application on the client computer. Check the Memory Exploit Mitigation logs to verify whether the application still runs.

Disabling Memory Exploit Mitigation

As a last result, you may want to disable Memory Exploit Mitigation for the following reasons:

- You have not been able to find which mitigation technique terminates an application that runs on the client. In this case, notify the Symantec Security Response. Symantec recommends that you reenable Memory Exploit Mitigation as soon as you finish troubleshooting.
- You do not want protection against software vulnerabilities.

To disable Memory Exploit Mitigation

1. In the console, click **Policies** > **Memory Exploit Mitigation**.
2. Uncheck **Enable Memory Exploit Mitigation**.
3. Click **OK**.

Reporting false positives to Security Response

If you suspect that a MEM detection is a false positive, contact Security Response to resolve the issue. Security Response needs to reproduce the false positive using the information that you provide.

To submit information about false positives to Security Response

1. In the Symantec Endpoint Protection Manager, make sure that Symantec Insight is enabled. Insight is enabled by default.

   Customizing Download Insight settings

2. Download and run the SymDiag tool on the client computer.

   Download SymDiag to detect Symantec product issues

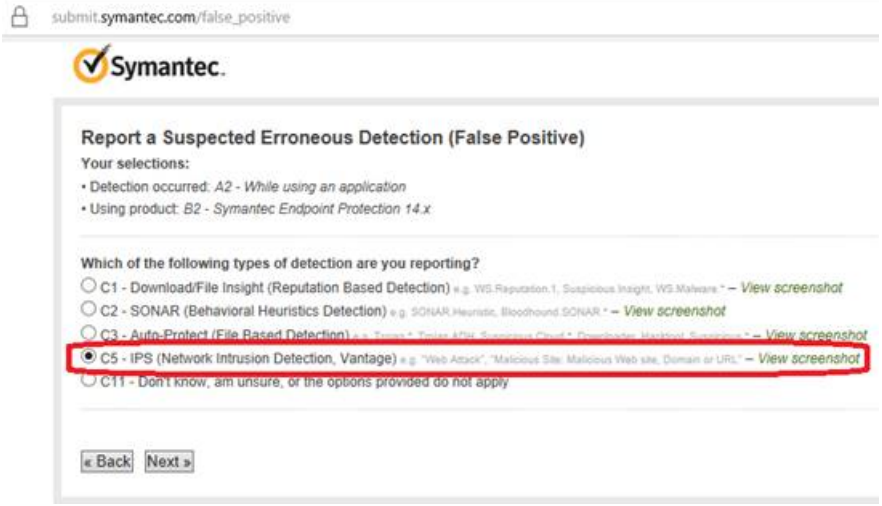
3. On the SymDiag tool **Home** page, click **Collect Data for Support**, and for the **Debug logging** > **Advanced** option, set the **WPP Debug** > **Trace Level** to **Verbose**.

   Use advanced debug logging options for the Symantec Endpoint Protection client in SymDiag

4. Reproduce the false positive detection.
5. After the log collection finishes, submit the `.sdbz` file to Technical Support by opening a new case or updating an existing case with this new information.

   Methods to provide data for Technical Support cases

6. Submit the detected application to the false positives portal, and do the following tasks:
   - Choose when the detection occurred, choose the **B2 Symantec Endpoint Protection 14.x** product, and click the **C5 - IPS** event.



- In the submission notes, provide the Technical Support case number from step 5, the application that triggered the MEM detection, and details about the application's version number.

  For example, you might add: "`"Blocked Attack: Return Oriented Programming API Invocation attack against C:\Program Files\VideoLAN\VLC\vlc.exe"`, the version for vlc.exe is 2.2.0-git-20131212-0038. This is not the latest available version but it is the version that our organization is required to use."

  Symantec Insider Tip: Successful Submissions!

7 On the client computer, compress a copy of the submissions folder that is located at: `%PROGRAMDATA%\Symantec\Symantec Endpoint Protection\CurrentVersion\Data\CmnClnt\ccSubSDK`.

Submit this folder to Technical Support and notify them of the tracking number for the false positive submission that you opened in step 6. Technical Support ensures that all necessary logs and materials are intact and associated with the false positive investigation.

Chapter 18

Managing Virus and Spyware Protection

This chapter includes the following topics:

- Managing the virus and spyware notifications that appear on client computers
- About the pop-up notifications that appear on Windows 8 clients
- Enabling or disabling Symantec Endpoint Protection pop-up notifications that appear on Windows 8 clients
- Managing early launch anti-malware (ELAM) detections
- Adjusting the Symantec Endpoint Protection early launch anti-malware (ELAM) options
- Configuring a site to use a private Insight server for reputation queries
- Configuring client groups to use private servers for reputation queries and submissions

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 18-1 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. See "Viewing the protection status of client computers" on page 247.
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 "How to update content and definitions on the clients" on page 178.

Table 18-1 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 436. 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 432. See "Setting up scheduled scans that run on Mac computers" on page 434. See "Setting up scheduled scans that run on Linux computers" on page 435.
Let clients upload critical events immediately	Make sure that clients (Windows only) can bypass the heartbeat interval and send critical events to the management server immediately. Critical events include any risk found (except cookies) and any intrusion event. You can find this option in **Clients > Policies > Communications Settings**. The option is enabled by default. Administrator notifications can alert you right away when the damper period for relevant notifications is set to **None**. See "Setting up administrator notifications" on page 671. **Note:** Only 12.1.4 and newer clients can send critical events immediately. Earlier clients send events at the heartbeat interval only.
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 440.

Table 18-1 Protecting computers from virus and spyware attacks *(continued)*

Task	Description
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 "Understanding server data collection and client submissions and their importance to the security of your network" on page 486.
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 page 377.
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 "Removing viruses and security risks" on page 404.

Removing viruses and security risks

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 18-2 Removing viruses and security risks

Step	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 406.

Table 18-2 Removing viruses and security risks *(continued)*

Step	Description
Step 2: Update definitions and rescan	You should make sure that clients use the latest definitions. For legacy clients that run on Windows computers, you should also make sure that your scheduled and on-demand scans use the Insight Lookup feature. As of 14, scheduled and on-demand scans always use Insight Lookup. 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 "How to update content and definitions on the clients" on page 178.
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 407.
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 Computer Status log to restart computers. See "Running commands on client computers from the console" on page 253.

Table 18-2 Removing viruses and security risks *(continued)*

Step	Description
Step 5: Investigate and clean remaining risks	If any risks remain, you should investigate them further. You can check the Symantec Security Response webpage 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 website from the scan results dialog box. You can also run Power Eraser from Symantec Endpoint Protection Manager to analyze and remediate difficult, persistent threats. Power Eraser is an aggressive analysis that you should run on one computer or a small number of computers only when the computers are unstable or heavily infected. See "What you should know before you run Power Eraser from the Symantec Endpoint Protection Manager console" on page 781. Symantec Technical Support also offers a Threat Expert tool that quickly provides detailed analysis of threats. You can also run a load point analysis tool that can help you troubleshoot problems. You run these tools directly on the client computer. See "Troubleshooting computer issues with the Symantec Diagnostic Tool (SymDiag)" on page 764.
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 655.

For more information, see Virus removal and troubleshooting on a network.

See "Preventing and handling virus and spyware attacks on client computers" on page 402.

See "Monitoring endpoint protection" on page 625.

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 "Removing viruses and security risks" on page 404.

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 "Removing viruses and security risks" on page 404.

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 480.

   If your policy is configured to use push mode, it is pushed out to the clients in the group at the next heartbeat.

   See "Updating policies and content on the client using push mode or pull mode" on page 165.
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.

Ransomware removal and protection with Symantec Endpoint Protection

What is ransomware?

Ransomware is a category of malware that sabotages documents and makes then unusable, but the computer user can still access the computer. Ransomware attackers force their victims to pay the ransom through specifically noted payment methods after which they may grant the victims access to their data. Unfortunately, ransomware decryption is not possible using removal tools.

Ransomlockers are a related type of malware that prevents users from accessing their devices or data by locking their computer. The victim receives a message that may appear to be from local law enforcement, demanding a "fine" to let victims avoid arrest and to unlock their computers.

How to remove ransomware

CryptoLocker is a ransomware variant where malware often encrypts a user's files and often deletes the original copy. The attacker requests a ransom for the files to be unencrypted. Not only are files on the local computer damaged, but also the files on any shared or attached network drives to which the computer has write access.

Organizations must respond to increasing threat of ransomware

Don't Pay That Ransom: Fighting Ransomware In A New Threat Landscape

Symantec Threat Landscape Round Up: Ransomware a US$34 million-a-year business

5 steps for preventing ransomware

Hardening Your Environment Against Ransomware

To avoid ransomware infection, follow these steps:

1. **Back up your computers and servers regularly.**

   Regularly back up the files on both the client computers and servers. Either back up the files when the computers are offline or use a system that networked computers and servers cannot write to. If you do not have dedicated backup software, you can also copy the important files to removable media. Then eject and unplug the removable media; do not leave the removable media plugged in.

2. **Lock down mapped network drives by securing them with a password and access control restrictions.**

   Use read-only access for files on network drives, unless it is absolutely necessary to have write access for these files. Restricting user permissions limits which files the threats can encrypt.

3. **Deploy and enable the following protections from Symantec Endpoint Protection Manager:**

   - **IPS**
     IPS blocks some threats that traditional virus definitions alone cannot stop. IPS is the best defense against drive-by downloads, which occurs when software is unintentionally downloaded from the Internet. Attackers often use exploit kits to deliver a web-based attack like CryptoLocker through a drive-by download.
     See "Enabling network intrusion prevention or browser intrusion prevention" on page 383.
   - **SONAR**

SONAR's behavioral-based protection is another crucial defense against malware. SONAR prevents the double executable file names of ransomware variants like CryptoLocker from running.

In a Virus and Spyware Protection policy, click **SONAR** > **Enable SONAR**.

- **Download Insight**

  Modify Download Insight in a **Virus and Spyware - High Security** policy to quarantine the files that have not yet been proven to be safe by the Symantec customer base.

  See "Preventing ransomware attacks with Download Insight" on page 411.

Recovering Ransomlocked Files Using Built-In Windows Tools

4. **Download the latest patches for web application frameworks, web browsers, and web browser plug-ins.**

   Attacking exploit kits cannot deliver drive-by downloads unless there is an old version of a plug-in to exploit, such as Flash. Historically, attacks were delivered through phishing and web browsers. Recently, more attacks are delivered through vulnerable web applications, such as JBOSS, WordPress, and Joomla.

5. **Use an email security product to handle email safely.**

   CryptoLocker is often spread through spam emails that contain malicious attachments. Scanning inbound emails for threats with a dedicated mail security product or service is critical to keep ransomware and other malware out of your organization. For important advice and recommendations, see:

   Support Perspective: W97M.Downloader Battle Plan

How to remove ransomware

There is no ransomware removal tool or CryptoLocker removal tool. Instead, if your client computers do get infected with ransomware and your data is encrypted, follow these steps:

1. **Do not pay the ransom.**

   If you pay the ransom:

   - There is no guarantee that the attacker will supply a method to unlock your computer or decrypt your files.
   - The attacker uses the ransom money to fund additional attacks against other users.

2. **Isolate the infected computer before the ransomware can attack network drives to which it has access.**

3. **Use Symantec Endpoint Protection Manager to update the virus definitions and scan the client computers.**

   New definitions are likely to detect and remediate the ransomware. Symantec Endpoint Protection Manager automatically downloads virus definitions to the client, as long as the client is managed and connected to the Symantec Endpoint Protection Manager.

In Symantec Endpoint Protection Manager, click **Clients**, right-click the group, and click **Run a command on the group** > **Update Content and Scan**.

4. **Restore damaged files from a known good backup.**

   As with other security products, Symantec Endpoint Protection cannot decrypt the files that ransomlockers have sabotaged.

5. **Submit the malware to Symantec Security Response.**

   If you can identify the malicious email or executable, submit it to Symantec Security Response. These samples enable Symantec to create new signatures and improve defenses against ransomware.

   Symantec Insider Tip: Successful Submissions!

For more information

- For major ransomware incidents, engage the Symantec Global Incident Response team. They can help you validate that you have been attacked and help you to decide what to do next. See:
  10 Ways Symantec Incident Response Can Help with Ransomware
  For help with an incident now:
  Email: incidentresponse@symantec.com
  Incident Response Hotline: (855) 378-0073
- Additional information about Ransomware threats

Preventing ransomware attacks with Download Insight

To prevent ransomware variants, configure Download Insight to quarantine the files that the Symantec customer base knows are malicious or that haven't yet been proven to be malicious.

See “Ransomware removal and protection with Symantec Endpoint Protection” on page 408.

To prevent ransomware attacks with Download Insight

1. In the console, open the **Virus and Spyware Protection policy - High Security** and click **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.
3. Check the following default options:
   - **Files with *5* or fewer users**
   - **Files known by users for *2* or fewer days**

   The low default values force the client to treat any file that has not been reported to Symantec by more than five users or for less than 2 days to be treated as unproven files. When unproven files meet these criteria, Download Insight detects the files as malicious.

4 Make sure that **Automatically trust any file downloaded from a trusted Internet or intranet site** is checked.

5 On the **Actions** tab, under **Malicious Files**, keep the first action as **Quarantine risk** and the second action as **Leave alone**.

6 Under **Unproven Files**, click **Quarantine risk**.

7 Click **OK**.

How Windows clients receive definitions from the cloud

Starting in 14, Symantec Endpoint Protection standard and embedded/VDI clients provide real-time protection with definitions in the cloud. Earlier versions provided some cloud protection with various features, such as Download Insight. Now, all virus and spyware features use the cloud to evaluate files. Cloud content includes the entire set of virus and spyware definitions as well as the latest information that Symantec has about files and potential threats.

Note: The Intelligent Threat Cloud Service is supported on Windows clients only.

Clients support cloud-enabled content

Cloud-enabled content includes a reduced-sized set of definitions that provides full protection. When the client requires new definitions, the client downloads or looks up the definitions in the cloud for better performance and speed.

Starting in 14, standard clients and embedded/VDI clients support cloud-enabled content.

See "How to choose a client installation type" on page 118.

All scans automatically use cloud lookups

Cloud lookups include queries to Symantec Insight for file reputation information and definition checking in the cloud.

- Scheduled and on-demand scans automatically perform cloud lookups.
- Auto-Protect also automatically performs cloud lookups. Auto-Protect now runs in user mode rather than kernel mode to reduce memory usage and provide better performance.

In addition to leveraging a smaller footprint with definitions on disk, the Intelligent Threat Cloud Service provides a 15-percent reduction in scan time.

Note: The 12.1.x Insight Lookup feature provides file reputation lookups for scheduled and on-demand scans of portal files on legacy clients. This option includes a separate sensitivity level. In version 14.0.x, 12.1.x clients use the sensitivity level that is set for Download Insight, and you can only enable or disable Insight Lookup.

Clients automatically send information about file reputation lookups to Symantec.

See "Managing the pseudonymous or non-pseudonymous data that clients send to Symantec" on page 489.

How cloud lookups work in your network

Symantec Endpoint Protection sends cloud lookups directly to the cloud.

Note: If you use an EDR server, reputation lookups are routed through the EDR server before they reach the cloud.

See "Configuring client groups to use private servers for reputation queries and submissions" on page 463.

If you want to use a proxy server, you can specify an HTTPS proxy in the client's browser Internet options. Or you can use the Symantec Endpoint Protection Manager console to specify the HTTPS proxy for clients in **Policies > External Communications**.

See "Specifying a proxy server for client submissions and other external communications" on page 491.

The amount of bandwidth that the Intelligent Threat Cloud Service clients use is nearly identical to pre-14 clients, which use reputation lookups only with specific features such as Download Insight.

How Symantec Endpoint Protection Manager alerts you about cloud lookup errors

If clients try cloud lookups for 3 days without success, by default Symantec Endpoint Protection Manager sends an email notification to system administrators. You can also view the alert in **Monitors > Logs> System Logs > Client Activity**. The notification condition type is **File Reputation Detection**.

See "Viewing logs" on page 655.

See "What are the types of notifications and when are they sent?" on page 663.

What are portal files?

Download Insight marks a file as a portal file when it examines a file that a user downloads from a supported portal. Scheduled and on-demand scans, Auto-Protect, and Download Insight evaluate the reputation of portal files using the sensitivity level that is set for Download Insight.

Note: Download Insight must be enabled to mark files as portal files.

Supported portals include: Internet Explorer, Firefox, Microsoft Outlook, Outlook Express, Google Chrome, Windows Live Messenger, and Yahoo Messenger. The portal list (or Auto-Protect portal list) is part of the Virus and Spyware Protection content that LiveUpdate downloads to the management server or the client.

Scans and Download Insight always evaluate non-portal files with a default internal sensitivity level that Symantec sets. The internal default detects only the most malicious files.

See "Managing Download Insight detections" on page 442.

An example of cloud lookups in action

An example of the way the Intelligent Threat Cloud Service protects clients:

- The client user runs Internet Explorer and tries to download a file. Download Insight uses its sensitivity level and reputation information from Symantec Insight in the cloud to determine that the file is not harmful.
- Download Insight determines that the file's reputation is acceptable, allows the file to download, and marks the file as a portal file.
- Later, Symantec gets more information about the file from its extensive global intelligence network. Symantec determines that the file might be harmful and updates the Insight reputation database. Symantec might provide a late-breaking signature for the file in its definitions in the cloud.
- If the user opens the file or runs a scan, Auto-Protect or the scan gets the latest information about the file from the cloud. Using the latest file reputation and the Download Insight sensitivity level, or using a late-breaking file signature, Auto-Protect or the scan now detects the file as potentially malicious.

Required and recommended settings

By default, Symantec Endpoint Protection uses the cloud. If you disable any of these options, you limit or disable cloud protection.

- Auto-Protect
  Auto-Protect must be enabled. Auto-Protect is enabled by default.
- Download Insight
  Download Insight must be enabled so that it can examine file downloads, and so that file downloads are marked as portal files for future scans. If you disable Download Insight, all file downloads are treated as non-portal. Scans detect only the most malicious non-portal files.
  See "Managing Download Insight detections" on page 442.
- Insight lookups

Insight lookups must be enabled. The Insight lookups option controls reputation lookups as well as cloud definition lookups. This option is enabled by default.

Warning: If you disable Insight lookups, cloud protection is completely disabled.

- Product usage and client submissions
  Symantec recommends that you allow your server and clients to share information with Symantec. Data you share with Symantec improves the performance of detection features. Information about the potential malware that might attack your computers helps improve the security landscape and address threats faster. Symantec makes every attempt to make the data pseudonymous to prevent the transmission of personally identifiable information.
  See "Understanding server data collection and client submissions and their importance to the security of your network" on page 486.

See "Symantec Endpoint Protection feature dependencies for Windows clients (12.1.x through 14.x)" on page 792.

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.

Starting in 14, scans access the complete definitions set in the cloud.

See "How Windows clients receive definitions from the cloud" on page 412.

Table 18-3 Modifying 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 418. See "About the default Virus and Spyware Protection policy scan settings" on page 427.

Table 18-3 Modifying scans on client computers *(continued)*

Task	Description
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. 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. **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 432. See "Setting up scheduled scans that run on Mac computers" on page 434. See "Setting up scheduled scans that run on Linux computers" on page 435. See "Running on-demand scans on client computers" on page 436.
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 to scan network drives. See "Customizing the virus and spyware scans that run on Windows computers" on page 466. See "Customizing the virus and spyware scans that run on Mac computers" on page 467. See "Customizing the virus and spyware scans that run on Linux computers" on page 468.
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 437.

Table 18-3 Modifying 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 440.
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 442.
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 495.
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 in Symantec Endpoint Protection" on page 544. See "About the files and folders that Symantec Endpoint Protection excludes from virus and spyware scans" on page 424.
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 for Windows clients" on page 452.
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 "Understanding server data collection and client submissions and their importance to the security of your network" on page 486.
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 456.

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.

Note: Starting in 14, scans access the complete definitions set in the cloud.

See "How Windows clients receive definitions from the cloud" on page 412.

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 415.

Table 18-4 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. Mac clients and Linux clients support Auto-Protect for the file system only. Starting in 14, on standard and embedded/VDI clients that are connected to the cloud, Auto-Protect automatically looks up the latest definitions in the cloud. See "Customizing Auto-Protect for Linux clients" on page 471.

Table 18-4 Scan types *(continued)*

Scan type	Description
Download Insight (Windows only)	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 Symantec Insight to make decisions about files" on page 446.
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 for Windows clients. You can schedule only a custom scan for Mac clients or Linux 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. If the Symantec Endpoint Protection client for Windows detects a large number of viruses, spyware, or high-risk threats, an aggressive scan mode engages. The scan restarts and uses Insight lookups. See "Setting up scheduled scans that run on Windows computers" on page 432. See "Setting up scheduled scans that run on Mac computers" on page 434.

Table 18-4 Scan types *(continued)*

Scan type	Description
SONAR (Windows only)	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. See "About SONAR" on page 493.
Early launch anti-malware (ELAM) (Windows only)	Works with the Windows early launch anti-malware driver. Supported only as of Windows 8 and Windows Server 2012. 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 459.

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 you use a server-based email scanning solution such as Symantec Mail Security, you might not need to enable Auto-Protect for email.

Mac clients and Linux clients do not support email Auto-Protect scans.

Table 18-5 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 those 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.
Microsoft Outlook Auto-Protect (Windows only)	Downloads incoming Microsoft Outlook email attachments and scans for viruses and security risks when the user reads the message and opens the attachment. Microsoft Outlook Auto-Protect supports Microsoft Outlook 98 through Outlook 2013, for the MAPI or Internet protocols. Microsoft Outlook Auto-Protect supports 32-bit and 64-bit systems. During installation, Symantec Endpoint Protection installs Microsoft Outlook Auto-Protect if you include it in the package and Microsoft Outlook is already installed on the computer. If a user downloads a large attachment over a slow connection, mail performance is affected. If you know the document is safe, you can create an exception. See "Excluding a file or a folder from scans" on page 552. **Note:** You should not install Microsoft Outlook Auto-Protect on a Microsoft Exchange Server. Instead you should install Symantec Mail Security for Microsoft Exchange.

Table 18-5 Types of Auto-Protect *(continued)*

Type of Auto-Protect	Description
Internet Email Auto-Protect (Windows only) This feature is only available for client versions earlier than 14.2 RU1.	Scans inbound Internet email body and email 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. Internet Email Auto-Protect supports 32-bit or 64-bit systems. 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. Email scanning does not support IMAP, AOL, or HTTP-based email such as Hotmail or Yahoo! Mail.
Lotus Notes Auto-Protect (Windows only) This feature is only available for client versions earlier than 14.2 RU1.	Scans incoming Lotus Notes email attachments for viruses and security risks. Lotus Notes Auto-Protect supports Lotus Notes 7.x or later. During installation, Symantec Endpoint Protection installs Lotus Notes Auto-Protect if you include it in the package and Lotus Notes is already installed on the computer.

See "About the types of scans and real-time protection" on page 418.

See "Customizing Auto-Protect for email scans on Windows computers" on page 472.

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.

You can change the action that Symantec Endpoint Protection takes when it detects a virus or a security risk. For Windows clients, 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 480.

You can view information about specific virus and security risks on the Symantec Security Response Web site.

Table 18-6 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.
Cookie	Messages that Web servers send to Web browsers for the purpose of identifying the computer or user.
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.
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.

Table 18-6 Viruses and security risks *(continued)*

Risk	Description
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 18-7 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 ■ Exchange 2013 ■ Exchange 2016 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 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 article, Configuring Symantec Endpoint Protection exclusions for Microsoft Forefront.

Table 18-7 File and folder exclusions *(continued)*

Files	Description
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.
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
Veritas products	The client automatically creates appropriate file and folder scan exclusions for certain Veritas products when they are detected. ■ Veritas Backup Exec ■ Veritas NetBackup ■ Veritas System Recovery
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.

Table 18-7 File and folder exclusions *(continued)*

Files	Description
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.
Trusted files	Virus and spyware scans use Insight, which 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 552.

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 18-8 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 ■ 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 18-8 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. 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 18-9 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. **Note:** The Aggressive option is likely to produce more false positives. This option is only recommended for advanced users.

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 18-10 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.
Microsoft Outlook Auto-Protect Internet Email Auto-Protect* Lotus Notes Auto-Protect* * Only available for client versions earlier than 14.2 RU1	Disabled
SONAR	Same as Virus and Spyware Protection Balanced 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 Balanced policy.

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 18-11 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.

Detections by SONAR are considered suspicious events. You configure actions for these detections as part of the SONAR configuration.

See "Managing SONAR" on page 495.

For Windows clients and Linux clients, 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: Risky cookies are always deleted unless you specify that you want to log cookies instead. You can specify only one action for cookies, either **Delete** or **Leave alone (log only)**.

Note: On Windows clients, 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 clients, you can specify whether 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 use different actions for scheduled, on-demand, or Auto-Protect scans.

See "Managing the Quarantine for Windows clients" on page 452.

How Symantec Endpoint Protection handles 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 Windows 8 clients" on page 458.

See "How Symantec Endpoint Protection handles detections of viruses and security risks" on page 430.

Setting up scheduled scans that run on Windows computers

You configure scheduled scans as part of a Virus and Spyware Protection policy.

Consider the following important points when you set up a scheduled scan for the Windows computers in your security network:

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 6 A.M., the scan runs at 6 A.M. The next scan is performed one week from Monday at 6 A.M. rather than the next Sunday at midnight. If you did not restart your computer until Tuesday at 6 A.M., 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.

Note: Windows settings include some options that are not available for clients that run on other operating systems.

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**.

See "Managing scans on client computers" on page 415.

See "Customizing administrator-defined scans for clients that run on Windows computers" on page 473.

See "Excluding file extensions from virus and spyware scans on Windows clients and Linux clients" on page 555.

Setting up scheduled scans that run on Mac computers

You configure scheduled scans as part of a Virus and Spyware Protection policy.

See "Managing scans on client computers" on page 415.

See "Customizing administrator-defined scans for clients that run on Mac computers" on page 474.

Note: Mac settings do not include all the options that are available for clients that run on Windows.

To set up scheduled scans that run on Mac computers

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 On the **Schedule** tab, under **Scanning schedule**, set the frequency and the time at which the scan should run.

8 If you want to save this scan as a template, check **Save a copy as a Scheduled Scan Template**.

9 Click **OK**.

Setting up scheduled scans that run on Linux computers

You configure scheduled scans as part of a Virus and Spyware Protection policy.

To set up scheduled scans that run on Linux computers

1 In the console, open a Virus and Spyware Protection policy.

2 Under **Linux Settings**, click **Administrator-defined Scans**.

3 On the **Scans** tab, under **Scheduled Scans**, click **Add**.

4 In the **Add Scheduled Scan** dialog box, click **Add Scheduled Scan**.

5 In the **Add Scheduled Scan** dialog box, on the **Scan Details** tab, type a name and description for this scheduled scan.

6 Under **Folder types**, click **Scan all folders** or specify the folders to scan.

7 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 or you create specific exceptions for the container file extensions.

---

8 Under **Additional options**, check or uncheck **Scan for security risks**.

9 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**.

10 Under **Missed Scheduled Scans**, you can disable the option to run a missed scan or you can change the retry interval.

11 If you want to save this scan as a template, check **Save a copy as a Scheduled Scan Template**.

12 Click **OK**.

See "Managing scans on client computers" on page 415.

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.

For Windows client computers, you can run an active, full, or custom on-demand scan. For Mac and Linux 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.

To run on-demand scans on client computers

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

2 Under **Clients**, right-click the group or clients that you want to scan.

3 Do one of the following actions:

- Click **Run a command on the group > Scan**.
- Click **Run command on computers > Scan**.

Click **Update Content and Scan** to update definitions and then run the scan in one step.

4 For Windows clients, select **Active Scan**, **Full Scan**, or **Custom Scan**, and then click **OK**.

See "Managing scans on client computers" on page 415.

See "Preventing and handling virus and spyware attacks on client computers" on page 402.

See "Running commands on client computers from the console" on page 253.

See "What are the commands that you can run on client computers?" on page 250.

Adjusting scans to improve computer performance

By default, virus and spyware scans 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).

Table 18-12 To adjust scans to improve computer 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 clients that run on Windows computers" on page 473.

Table 18-12 To adjust scans to improve computer performance on Windows computers *(continued)*

Task	Description
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 432.
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 that the file cache is enabled (the default is enabled). When the file cache is enabled, Auto-Protect remembers the clean files that it scanned and does not rescan them. ■ **Network settings** When Auto-Protect scans of remote computers are enabled, make sure that **Only when files are executed** is enabled. See "Customizing Auto-Protect for Windows clients" on page 468.
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 477.

Table 18-12 To adjust scans to improve computer performance on Windows computers *(continued)*

Task	Description
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 Windows clients" on page 477.
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 use Shared Insight Cache for scheduled and manual scans on your client computers. Shared Insight Cache is a separate application that you install on a server or in a virtual environment. See "Enabling the use of a network-based Shared Insight Cache" on page 682.
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 459.

Table 18-13 To adjust scans to improve computer performance on Mac computers

Task	Description
Enable idle-time scan	Applies to scheduled scans on clients that run on Mac computers. This option configures scheduled scans to run only while the computer is idle. See "Customizing administrator-defined scans for clients that run on Mac computers" on page 474.
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 470.

Table 18-14 To adjust scans to improve computer performance on Linux computers

Task	Description
Scan by type of folder	The default is to scan all folder types. You can specify any of: **Root, Home, Bin, Usr, Etc**, and **Opt**. If you know that a folder is safe, you can uncheck it in the list.

Table 18-14 To adjust scans to improve computer performance on Linux computers *(continued)*

Task	Description
Scan by file type	The default is to scan all files. If you know that a given extension is safe, you can remove it from the list.
Scan files inside compressed files	You can expand up to three levels to scan within compressed files. You might want to change the level to 1 or 2 to reduce scan time.
Scan for security risks	Lets you choose whether to scan for security risks. Security risks are updated through LiveUpdate. Scanning for security risks slows the scan down, but increases security. The default is to scan for security risks. To improve computer performance, uncheck this option.

See "Managing scans on client computers" on page 415.

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 and Linux computers.

Note: If you increase the protection on your client computers, you might affect computer performance.

Table 18-15 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.

Table 18-15 Adjusting scans to increase protection on Windows computers *(continued)*

Task	Description
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 on 12.1.6.x and earlier clients Insight Lookup uses the latest definition set from the cloud and information from the Insight reputation database to scan and make decisions about files that were downloaded from a supported portal. In 12.1.6.x and earlier versions, you can configure the Insight Lookup sensitivity as well as enable or disable Insight Lookup. As of version 14, you can only enable or disable Insight Lookup for 12.1.6.x clients. **Warning:** Make sure that Insight Lookup is enabled. If you disable Insight lookups, cloud protection is completely disabled. In 14, scheduled and on-demand scans always use the cloud to evaluate portal files. Auto-Protect also uses the cloud to evaluate portal files. See "Customizing administrator-defined scans for clients that run on Windows computers" on page 473. See "How Windows clients receive definitions from the cloud" on page 412.
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 480.
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 477.

Table 18-15 Adjusting scans to increase protection on Windows computers *(continued)*

Task	Description
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. See "Customizing Auto-Protect for Windows clients" on page 468.

Table 18-16 Adjusting scans to increase protection on Mac and Linux computers

Task	Description
Modify compressed file options for scans	The default is to scan 3 levels deep in compressed files. To increase protection, leave it at 3 levels, or change it to 3 if it is at a lower level. See "Customizing administrator-defined scans for clients that run on Mac computers" on page 474. See "Customizing administrator-defined scans for clients that run on Linux computers" on page 475.
Lock Auto-Protect settings	Some settings are locked by default; you can lock additional settings so that users cannot change the protection on their computers. On the Mac client and the Linux client, you can click **Enable Auto-Protect**, and then click the lock icon to lock the setting. See "Customizing Auto-Protect for Mac clients" on page 470. See "Customizing Auto-Protect for Linux clients" on page 471.
Specify stronger scan detection actions	Specify **Quarantine** or **Delete** (Linux only) actions for detections. **Note:** Be careful when you use **Delete** 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 480.

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 415.

Table 18-17 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 Symantec Insight to make decisions about files" on page 446.
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 671. 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 649.

Table 18-17 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 Windows clients" on page 556. See "Excluding a trusted web domain from scans on Windows clients" on page 557. **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 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 "Customizing Download Insight settings" on page 479.

Table 18-17 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 Files folder. Typically, the folder location is one of the following: ■ Windows 8 and later: *Drive*:\Users*username*\AppData\Local\Microsoft\Windows\INetCache ■ Windows Vista / 7: *Drive*:\Users*username*\AppData\Local\Microsoft\Windows\Temporary Internet Files ■ Windows XP (for legacy 12.1.x clients): *Drive*:\Documents and Settings*username*\Local Settings\Temporary Internet Files See "Customizing Download Insight settings" on page 479.

Table 18-17 Managing Download Insight detections *(continued)*

Task	Description
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 "Managing the pseudonymous or non-pseudonymous data that clients send to Symantec" on page 489.

How Symantec Endpoint Protection uses Symantec Insight 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 is available to Symantec products in the cloud through Symantec Insight. Symantec Insight provides a file reputation database and the latest virus and spyware definitions.

Symantec products leverage Insight 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. Symantec Endpoint Protection must request or query Insight for information. The queries are called reputation lookups, cloud lookups, or Insight lookups.

Insight reputation ratings

Symantec Insight determines each file's level of risk or security rating. The rating is also known as the file's reputation.

Insight determines a file's security rating by examining the following characteristics of a 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

Insight lookups

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 requires reputation information to make detections. SONAR also uses reputation information to make detections.

You can change the Insight lookups setting on the **Clients** tab. Go to **Policies > Settings > External Communications > Client Submissions**.

Starting in 14, on standard and embedded/VDI clients, the Insight lookups option also allows Auto-Protect and scheduled and manual scans to look up file reputation information as well as definitions in the cloud. Symantec recommends that you keep the option enabled.

Warning: Download Insight, SONAR, and virus and spyware scans use Insight lookups for threat detection. Symantec recommends that you always allow Insight lookups. Disabling lookups disables Download Insight and impairs the functionality of SONAR heuristics and virus and spyware scans.

See "Symantec Endpoint Protection feature dependencies for Windows clients (12.1.x through 14.x)" on page 792.

File reputation submissions

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 and the latest definitions in the cloud. The more clients that submit information the more useful the reputation database becomes.

Symantec recommends that you keep client submissions for reputation detections enabled.

See "Managing Download Insight detections" on page 442.

See "Understanding server data collection and client submissions and their importance to the security of your network" on page 486.

See "Configuring a site to use a private Insight server for reputation queries" on page 462.

How does Symantec Endpoint Protection use advanced machine learning?

How does advanced machine learning work?

The advanced machine learning (AML) engine determines if a file is good or bad through a learning process. Symantec Security Response trains the engine to recognize malicious

attributes and defines the rules that the AML engine uses to make detections. Symantec trains and tests the AML engine in a lab environment using the following process:

- LiveUpdate downloads the AML model to the client and runs for several days.
- The AML engine learns which applications the client runs and get exploited using the client's telemetry data. Each client computer is part of the global intelligence network that returns information about the model to Symantec.
- Symantec adjusts the AML model based on what Symantec learns from the clients' telemetry data.
- Symantec modifies the AML model to block the applications that exploits typically attack.

AML is part of the static data scanner (SDS) engine. The SDS engine includes the emulator, the Intelligent Threat Cloud Service (ITCS), and the CoreDef-3 definitions engine.

Symantec Endpoint Protection uses advanced machine learning in Download Insight, SONAR, and virus and spyware scans, all which use Insight lookups for threat detection.

How does AML work with the cloud?

Symantec leverages the Intelligent Threat Cloud Service (ITCS) to confirm the detection that AML makes on the client computer is correct. Sometimes AML may reverse the conviction after it checks with the ITCS. While the AML engine does not need Symantec Insight, this feedback enables Symantec to train the AML algorithms to reduce false positives and increase true positives. When the computer is online, Symantec Endpoint Protection can stop an average of 99% of threats.

See “How Windows clients receive definitions from the cloud” on page 412.

See “How does the emulator in Symantec Endpoint Protection detect and clean malware?” on page 450.

How do I configure AML?

You cannot configure advanced machine learning. LiveUpdate downloads the AML definitions by default. However, you do need to make sure that the following technologies are enabled.

Table 18-18 Steps to ensure that AML protects the client computers

Task	Description
Step 1: Make sure that cloud lookup availability is enabled	The queries that AML makes to Symantec Insight are called reputation lookups, cloud lookups, or Insight lookups. If Insight lookups are enabled, the AML detections for SONAR and virus and spyware scans have fewer false positives. To verify that Insight lookups are enabled, see: See "How Symantec Endpoint Protection uses Symantec Insight to make decisions about files" on page 446. In addition, make sure that client submissions are enabled. This information helps Symantec measure and improve the effectiveness of detection technologies. See "Understanding server data collection and client submissions and their importance to the security of your network" on page 486.
Step 2: Make sure that Bloodhound Detections are enabled	Set the Bloodhound Detection level to either automatic or aggressive. See "Modifying global scan settings for Windows clients" on page 477. When the AML engine encounters certain high-risk files, the client automatically engages a more aggressive scan. When aggressive scan mode engages: ■ The scan restarts. ■ The following notification appears on the client: `Running an aggressive scan that uses Insight lookups to clean your computer.` In the aggressive mode, you may need to further manage the false positives.
Step 3: Make sure that LiveUpdate downloads high intensity definitions (14.0.1) (optional)	LiveUpdate always downloads AML content. As of 14.0.1, LiveUpdate downloads a more aggressive set of definitions that work with the low bandwidth policy you get from the cloud. You can disable AML content from being downloaded through LiveUpdate. From LiveUpdate to Symantec Endpoint Protection Manager: See "Downloading content from LiveUpdate to the Symantec Endpoint Protection Manager" on page 186. From Symantec Endpoint Protection Manager to the Windows clients: See "Reverting to an older version of the Symantec Endpoint Protection security updates" on page 213. See "About the types of content that LiveUpdate downloads" on page 191.

Table 18-18 Steps to ensure that AML protects the client computers *(continued)*

Task	Description
Step 4: Handle false positives	Manage the false positives using the Exceptions policy. See "Creating exceptions for Virus and Spyware scans" on page 548. See "Handling and preventing SONAR false positive detections" on page 497. Best Practice when Symantec Endpoint Protection is Detecting a File that is Believed to be Safe

Troubleshooting advanced machine learning

The logs and reports for advanced machine learning detections are the same as for the other SDS engines. To see a report with recent threats, run a Risk report for **New Risks Detected in the Network**.

As of 14.0.1, you can run a scheduled report for AML detections. On the **Reports** page, click **Scheduled Reports** > **Add** > **Computer Status** > **Advanced Machine Learning (Static) Content Distribution**. The Symantec Endpoint Protection Manager domain must be enrolled in the cloud console for the report to appear.

See "How to run scheduled reports" on page 652.

See "Viewing logs" on page 655.

How does the emulator in Symantec Endpoint Protection detect and clean malware?

Symantec Endpoint Protection 14 introduced a powerful new emulator to protect against malware from custom packer attacks. For Auto-Protect and virus scans, this emulator improves scan performance and effectiveness by at least 10 percent from previous releases. This anti-evasion technique addresses packed malware obfuscation techniques and detects the malware that is hidden inside custom packers.

What are custom packers?

Many malware programs make use of "packers," or the software programs that are used to compress and encrypt files for transport. These files are then executed in memory upon arrival on the user's computer.

While packers themselves are not malware, attackers use them to hide malware and obfuscate the code's real intention. Once the malware is unpacked, it executes and launches its malicious payload, often bypassing firewalls, gateways, and malware protection. Attackers have shifted from using commercial packers (such as UPX, PECompact, ASProtect, and Themida) to

creating custom packers. The custom packers use proprietary algorithms to bypass standard detection techniques.

Many of the emerging custom packers are polymorphic. They use an anti-detection strategy whereby the code itself changes frequently, but the purpose and functionality of the malware remains the same. Custom packers also use clever ways of injecting the code into a target process and change its execution flow, frequently throwing off unpacker routines. Some of them are computationally intensive, calling special APIs that make the unpacking difficult.

Custom packers have grown increasingly sophisticated to hide the attack until it's too late.

How does the Symantec Endpoint Protection emulator protect against custom packers?

The high-speed emulator in Symantec Endpoint Protection fools malware into thinking it runs on the regular computer. Instead, the emulator unpacks and detonates the custom-packed file in a lightweight virtual sandbox on the client computer. The malware then opens up its payload in full, causing threats to reveal themselves in a contained environment. A static data scanner, which includes the antivirus engine and heuristics engine, acts on the payload. The sandbox is ephemeral and goes away after the threat is dealt with.

The emulator requires sophisticated technology that mimics operating systems, APIs, and processor instructions. It simultaneously manages the virtual memory and runs various heuristics and detection technologies to examine the payload. It takes an average of 3.5 milliseconds for clean files and 300 milliseconds for malware, at about the same time it takes client users to click a file on their desktop. The emulator can detect threats quickly with minimal performance and productivity impact, so client users are not interrupted. In addition, the emulator uses a minimal amount of disk space, a maximum of 16 MB memory in the virtual environment.

The emulator works with other protection techniques, which include advanced machine learning, memory exploit mitigation, behavior monitoring, and reputation analysis. Sometimes multiple engines come into play, collaborating in a response to prevent, detect, and remediate attacks.

The emulator does not use the Internet. However, the engines within the static data scanner may require the Internet based on the malware that the emulator extracted out of the custom packer.

See "How does Symantec Endpoint Protection use advanced machine learning?" on page 447.

How do I configure the emulator?

The emulator is built into the Symantec Endpoint Protection software so you don't need to configure it. Symantec regularly adds or changes the emulator content for new threats and releases quarterly content updates to the emulator engine. By default, LiveUpdate automatically downloads this content with the virus and spyware definitions.

See "Downloading content from LiveUpdate to the Symantec Endpoint Protection Manager" on page 186.

Symantec Endpoint Protection Manager does not include separate logs for the detections that the emulator makes. Instead, you can find any detections in the Risk log and Scan log.

See "Viewing logs" on page 655.

Managing the Quarantine for Windows clients

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 415.

Table 18-19 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 455.
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 Windows clients handle quarantined items" on page 454.

Table 18-19 Managing the Quarantine *(continued)*

Task	Description
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 453. ■ 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 "Specifying when repaired files, backup files, and quarantined files are automatically deleted" on page 454.
Collect information about quarantined items	You can configure the client to forward infected or suspicious files and related side effects to a Central Quarantine Server for further analysis. You can use this information to refine its detection and repair. You can enable signature-based detections in the quarantine to be forwarded from the local quarantine to an existing Central Quarantine Server. Reputation detections in the local quarantine cannot be sent to a Central Quarantine Server. See "Configuring how Windows clients handle quarantined items" on page 454.

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 for Windows clients" on page 452.

To specify a local Quarantine folder

1. On the **Virus and Spyware Protection Policy** page, under **Windows Settings**, click **Quarantine**.
2. On the **General** 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 Click **OK**.

Specifying when repaired files, backup files, and quarantined files are automatically deleted

Symantec Endpoint Protection automatically deletes repaired files, backup files, and quarantined files 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 for Windows clients" on page 452.

To specify when repaired files, backup files, and quarantined files are automatically deleted

1 In the console, open a Virus and Spyware Protection policy and under **Windows Settings**, click **Quarantine**.

2 On the **Cleanup** tab, check or uncheck the options to enable or disable them, and configure the time interval and size maximums.

3 Click **OK**.

Configuring how Windows clients handle quarantined items

You can configure the actions that you want to take when new definitions arrive on Symantec Endpoint Protection client computers. By default, the client rescans items in the Quarantine and automatically repairs and restores items silently. If you created an exception for a file or application in the Quarantine, Symantec Endpoint Protection restores the file after new definitions arrive.

In addition, you can configure clients to automatically submit quarantined items to a Central Quarantine Server. You use this central repository to add the threat samples that you detect in your environment. You can use that information to set up "red team" attacks to strengthen your security.

Note: Version 14 does not include the Quarantine Server and Quarantine Console. You can install these tools from the installation disc in an earlier version.

See "Managing the Quarantine for Windows clients" on page 452.

See “Removing viruses and security risks” on page 404.

To configure how Windows clients handle quarantined items

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 options.
3. To submit quarantined items to the Central Quarantine Server, check **Allow client computers to automatically submit quarantined items to a Quarantine Server**, and specific the server name and port number.
4. 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.

See “Managing scans on client computers” on page 415.

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 **Additional 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 415.

Table 18-20 Tasks for managing virus and spyware notifications that appear on client computers

Task	Description
Customize a scan detection message	For Windows and Linux client computers, you can configure a detection message for the following types of scans: ■ All types of Auto-Protect ■ 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, to on-demand scans, and to Auto-Protect detections. These notification messages appear in the macOS Notification Center. You cannot customize the messages for Mac. See "Customizing administrator-defined scans for clients that run on Windows computers" on page 473. See "Customizing administrator-defined scans for clients that run on Mac computers" on page 474. See "Customizing administrator-defined scans for clients that run on Linux computers" on page 475.
Change settings for user notifications about Download Insight detections	Applies to Windows client computers only. You can change the notifications that users receive about Download Insight detections. See "Managing Download Insight detections" on page 442.

Table 18-20 Tasks for managing virus and spyware notifications that appear on client computers *(continued)*

Task	Description
Change settings for user notifications about SONAR detections	Applies to Windows client computers only. You can change the notifications that users receive about SONAR detections. See "Managing SONAR" on page 495.
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 clients that run on Windows computers" on page 473.
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. Internet Email Auto-Protect is available only to client versions earlier than 14.2 RU1. See "Customizing Auto-Protect for email scans on Windows computers" on page 472.
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 Windows computers" on page 482.
Configure warnings, errors, 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 log handling and notification settings on Windows computers" on page 478.

Table 18-20 Tasks for managing virus and spyware notifications that appear on client computers *(continued)*

Task	Description
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 that appear on Windows 8 clients" on page 459.

About the pop-up notifications that appear on Windows 8 clients

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 that appear on Windows 8 clients" on page 459.

See "How Symantec Endpoint Protection handles detections on Windows 8 computers" on page 432.

Enabling or disabling Symantec Endpoint Protection pop-up notifications that appear 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 that appear 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 Windows 8 clients" on page 458.

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.

Note: ELAM is only supported on Microsoft Windows 8 or later, and Windows Server 2012 or later.

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 documentation for more information.

Table 18-21 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 655.
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 655.
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 461. See "Adjusting scans to improve computer performance" on page 437.
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 461.

Table 18-21 Managing ELAM detections *(continued)*

Task	Description
Run Power Eraser on ELAM detections that Symantec Endpoint Protection cannot remediate	In some cases, an ELAM detection requires Power Eraser. In those cases, a message appears in the log suggesting that you run Power Eraser. You can run Power Eraser from the console. Power Eraser is also part of the Symantec Help tool. You should run Power Eraser in rootkit mode. See "Starting Power Eraser analysis from Symantec Endpoint Protection Manager" on page 788. See "Troubleshooting computer issues with the Symantec Diagnostic Tool (SymDiag)" on page 764.

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 as of Microsoft Windows 8 and Windows Server 2012.

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 or the registry editor to view and modify the Windows ELAM settings. See your Windows 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 459.

See "Troubleshooting computer issues with the Symantec Diagnostic Tool (SymDiag)" on page 764.

Configuring a site to use a private Insight server for reputation queries

Private Insight server settings let you direct client reputation queries to an intranet server, if you have purchased and installed Symantec Insight for Private Clouds. Symantec Insight for Private Clouds is typically installed in networks that lack Internet connectivity. The private Insight server stores a copy of Symantec Insight's reputation database. Symantec Endpoint Protection reputation queries are handled by the private Insight server rather than Symantec's Insight server.

The private server downloads the Symantec Insight data over an encrypted, secure connection. You can manually update the Insight data or use third-party tools to check for updates and download the data automatically. Your update method depends on your network and the type of server on which you run Symantec Insight for Private Clouds.

When you use a private Insight server, Symantec does not receive any queries or submissions for file reputation.

To configure a site to use a private Insight server for reputation queries

1 In the console, on the **Admin** page, select **Servers**.

2 Select the site, and then under **Tasks**, select **Edit Site Properties**.

3 On the **Private Insight Server** tab, make sure that you check **Enable private Insight server**.

You must also enter the **Name**, **Server URL**, and **Port** number.

Note: If you change an existing Server URL to an invalid URL, clients use the previously valid URL for the private Insight server. If the Server URL has never been configured and you enter an invalid URL, clients use the default Symantec Insight server.

At the next heartbeat, your clients start to use the specified private server for reputation queries.

See "How Symantec Endpoint Protection uses Symantec Insight to make decisions about files" on page 446.

See “Configuring client groups to use private servers for reputation queries and submissions” on page 463.

Configuring client groups to use private servers for reputation queries and submissions

You can direct client reputation queries (Insight lookups) from a group to a private intranet server. The private server can be the Symantec Endpoint Detection and Response appliance or the Symantec Insight for Private Clouds server that you purchase and install separately in your network.

The following are the private server options for groups:

- Symantec Endpoint Detection and Response
  Symantec EDR servers gather data about client detections and provide forensic analysis. When you use a Symantec EDR server, Symantec Endpoint Protection sends all reputation queries (lookups) and most types of client submissions to Symantec EDR. Symantec EDR then sends the queries or submissions to Symantec. Note that Symantec EDR receives antivirus, SONAR, and IPS submissions, but it does not receive file reputation submissions. Symantec Endpoint Protection always sends file reputation submissions directly to Symantec.
- Symantec Insight for Private Clouds
  This option redirects the reputation queries from clients in the group to a private Insight server. The private Insight server stores a copy of Symantec's Insight reputation database. The private Insight server handles the reputation queries rather than Symantec’s Insight server. When you use a private Insight server, clients continue to send submissions about detections to Symantec. Typically, you use a private Insight server in a dark network, which is a network that is disconnected from the Internet. In that case, Symantec cannot receive any client submissions.

See “Understanding server data collection and client submissions and their importance to the security of your network” on page 486.

You can also copy the private server configuration to other client groups.

You can specify multiple private servers to load balance network traffic. You can also specify multiple groups of servers to manage failover.

When you choose to enable an EDR server, the EDR connection status appears in the client user interface as well as the management console logs and reports. To communicate with the EDR server, the Symantec Endpoint Protection client must at a minimum run Virus and Spyware Protection.

Note: If you enable private servers for groups, 12.1.5 and earlier clients in those groups cannot use Symantec servers if the designated private server is not available. 12.1.5 and earlier clients cannot use the priority list and must be configured to use a single server.

To configure client groups to use a private server

1. In the console, go to **Clients** and select the group that should use the private server list.
2. On the **Policies** tab, click **External Communications Settings**
3. On the **Private Cloud** tab, click **Enable private servers to manage my data**.
4. Depending on which type of server you use, click **Use an Advanced Threat Protection server for Insight lookups and submissions** or **Use a private Insight server for Insight lookups**.

   You should not mix server types in the priority list.
5. Click **Use Symantec servers when private servers are not available** if you want clients to use Symantec servers for reputation queries and client antivirus and SONAR submissions.

   Clients always send file reputation submissions to Symantec.
6. Under **Private Servers**, click **Add > New Server**.
7. In the **Add Private Server** dialog, select the protocol and then enter the host name for the URL.
8. Specify the port number for the server.
9. To designate this server as the single server that 12.1.5 and earlier clients use, click **Use this server as the private Insight server for 12.1.5 clients and earlier**. The 12.1.5 and earlier clients cannot use a server list, so you must specify which server these legacy clients should use.
10. To add a priority group, click **Add > New Group**.
11. To apply the settings to additional client groups, click **Copy settings**. Select the groups and locations, and then click **OK**.

Chapter 19

Customizing scans

This chapter includes the following topics:

- Configuring Windows Security Center notifications to work with Symantec Endpoint Protection clients

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.

Table 19-1 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 the **Scan Results** dialog for Auto-Protect scans of the file system. See "Customizing Auto-Protect for Windows clients" on page 468. See "Customizing Auto-Protect for email scans on Windows computers" on page 472.
Customize administrator-defined scans	You can customize the following types of options for scheduled and on-demand scans. ■ Compressed files ■ Tuning options ■ Advanced schedule options ■ User notifications about detections See "Customizing administrator-defined scans for clients that run on Windows computers" on page 473. 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 459.

Table 19-1 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 479.
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 480.
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 477.
Customize miscellaneous options for Virus and Spyware Protection	You can specify the types of risk events that clients send to Symantec Endpoint Protection Manager. See "Modifying log handling and notification settings on Windows computers" on page 478.

See "Managing scans on client computers" on page 415.

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.

Table 19-2 Customizing virus and spyware scans 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 470.
Customize administrator-defined scans	You can customize common settings and notifications as well as scan priority. You can also enable 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 474.

Customizing the virus and spyware scans that run on Linux computers

You can customize options for administrator-defined scans (scheduled and on-demand scans) that run on Linux computers. You can also customize options for Auto-Protect.

Table 19-3 Customizing virus and spyware scans on Linux 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 Linux clients" on page 471.
Customize administrator-defined scans	You can customize the following types of options for scheduled and on-demand scans. ■ File and folder types ■ Compressed files ■ Security risks ■ Scheduling options ■ User notifications You can also customize scan actions.
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 480.
Customize miscellaneous options for Virus and Spyware Protection	You can specify the types of risk events that clients send to Symantec Endpoint Protection Manager. See "Modifying log handling settings on Linux computers" on page 479.

Customizing Auto-Protect for Windows clients

You might want to customize Auto-Protect settings for Windows clients.

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, make sure that **Enable Auto-Protect** is checked.

Warning: If you disable Auto-Protect, Download Insight cannot function even if it is enabled.

4 Under **Scanning**, under **File types**, select 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 480.

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 456.

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**.

See "Customizing the virus and spyware scans that run on Windows computers" on page 466.

See "Managing scans on client computers" on page 415.

Customizing Auto-Protect for Mac clients

You might want to customize Auto-Protect settings for the clients that run on Mac computers.

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 552.

---

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**.

See "Customizing the virus and spyware scans that run on Mac computers" on page 467.

See "Changing the action that Symantec Endpoint Protection takes when it makes a detection" on page 480.

See "Managing the virus and spyware notifications that appear on client computers" on page 456.

Customizing Auto-Protect for Linux clients

You might want to customize Auto-Protect settings for the clients that run on Linux computers.

To customize Auto-Protect for Linux clients

1. In the console, open a Virus and Spyware Protection policy.
2. Under **Linux Settings**, under **Protection Technology**, click **Auto-Protect**.
3. On the **Scan Details** tab, check or uncheck **Enable Auto-Protect**.
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 compressed files.
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. 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 480.

   You can also set remediation options for Auto-Protect.
10. On the **Notifications** tab, set any of the notification options.

    See "Managing the virus and spyware notifications that appear on client computers" on page 456.

11 On the **Advanced** tab, check or uncheck **Enable the cache**. Set a cache size or accept the default.

12 Click **OK**.

See "Customizing the virus and spyware scans that run on Linux computers" on page 468.

See "Changing the action that Symantec Endpoint Protection takes when it makes a detection" on page 480.

See "Managing the virus and spyware notifications that appear on client computers" on page 456.

Customizing Auto-Protect for email scans on Windows computers

You can customize Auto-Protect for email scans on Windows computers.

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**, select one of the following options:

- **Microsoft Outlook Auto-Protect**
- **Internet Email Auto-Protect***
- **Lotus Notes Auto-Protect***

* Only available for client versions earlier than 14.2 RU1.

3 On the **Scan Details** tab, check or uncheck **Enable Internet Email Auto-Protect**.

4 Under **Scanning**, under **File types**, select 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 480.

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**.

See "Customizing the virus and spyware scans that run on Windows computers" on page 466.

See "Managing the virus and spyware notifications that appear on client computers" on page 456.

Customizing administrator-defined scans for 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.

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**:

- 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.
- On the **Tuning** tab, change the tuning level for the best client computer performance or the best scan performance.

Click **OK** to save changes.

5 On the **Scan Details** tab, you can enable or disable Insight Lookup for legacy 12.1.x clients only.

6 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.

7 On the **Actions** tab, change any detection actions.

See "Changing the action that Symantec Endpoint Protection takes when it makes a detection" on page 480.

8 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 456.

9 Click **OK**.

See "Customizing the virus and spyware scans that run on Windows computers" on page 466.

See "Setting up scheduled scans that run on Windows computers" on page 432.

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.

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.

For a new scan, you can create a new scan manually, or create a scheduled scan from a template.

4 On the **Scan Details** tab, under **Scan drives and folders**, select the items that you want to scan.

5 You can also enable or disable idle-time scans. Enabling the option improves computer performance; disabling the option improves scan performance.

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 on the client.

5 Click **OK**.

See "Customizing the virus and spyware scans that run on Mac computers" on page 467.

See "Setting up scheduled scans that run on Mac computers" on page 434.

See "Changing the action that Symantec Endpoint Protection takes when it makes a detection" on page 480.

See "Managing the virus and spyware notifications that appear on client computers" on page 456.

Customizing administrator-defined scans for clients that run on Linux computers

You might want to customize scheduled or on-demand scans for the clients that run on Linux computers. You can set options for scans of compressed files and optimize the scan for computer or scan performance.

To customize an administrator-defined scan for the clients that run on Linux computers

1. In the console, open a Virus and Spyware Protection policy.
2. Under **Linux 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, check **Scan all folders** or specify the particular folders you want to scan.
5. Click **Scan all files** or **Scan only selected extensions** and specify the extensions you want to scan.
6. On the **Scan files inside compressed files** choice, you can reduce the number of levels to scan compressed files. If you reduce the number of levels, you might improve client computer performance.
7. Check or uncheck **Scan for security risks**.
8. For scheduled scans only, on the **Schedule** tab, set any of the following options:
   - **Scanning schedule**
     You can set how often the scan runs, on a daily, weekly, or monthly basis.
   - **Missed Scheduled Scans**
     You can specify a retry interval for missed scans.
9. On the **Actions** tab, change any detection actions.

   See "Changing the action that Symantec Endpoint Protection takes when it makes a detection" on page 480.
10. 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 456.
11. Click **OK**.

See "Customizing the virus and spyware scans that run on Linux computers" on page 468.

See "Setting up scheduled scans that run on Linux computers" on page 435.

See "Changing the action that Symantec Endpoint Protection takes when it makes a detection" on page 480.

See "Managing the virus and spyware notifications that appear on client computers" on page 456.

Randomizing scans to improve computer performance in virtualized environments on Windows clients

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 P.M. If you select a four-hour time interval, scans on client computers start at a randomized time between 8:00 P.M. and 12:00 A.M.

To randomize scans to improve computer performance in virtualized environments

1. In the console, open a Virus and Spyware Protection policy.
2. Under **Windows Settings**, click **Administrator-defined Scans**.
3. Create a new scheduled scan or select an existing scheduled scan to edit.
4. In the **Add Scheduled Scan** or **Edit Scheduled Scan** dialog box, click the **Schedule** tab.
5. Under **Scanning Schedule**, select how often the scan should run.
6. 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.
7. Make sure that you enable **Randomize scan start time within this period (recommended in VMs)**.
8. Click **OK**.
9. Make sure that you apply the policy to the group that includes the computers that run Virtual Machines.

See "Adjusting scans to improve computer performance" on page 437.

See "Setting up scheduled scans that run on Windows computers" on page 432.

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 415.

See "Customizing the virus and spyware scans that run on Windows computers" on page 466.

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 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 the level of 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 log handling and notification settings 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.

You can set the following options:

- Specify a default URL that Symantec Endpoint Protection uses when it repairs a security risk that changed a browser home page.
- Specify Risk log handling options.
- Warn users when definitions are out-of-date or missing.
- Exclude virtual images from Auto-Protect or administrator-defined scans.

To modify log handling and notification settings on Windows computers

1. In the console, open a Virus and Spyware Protection policy.
2. Under **Windows Settings**, click **Miscellaneous**.

   Specify options for **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.

See "Customizing the virus and spyware scans that run on Windows computers" on page 466.

5 Click **OK**.

See "Managing the virus and spyware notifications that appear on client computers" on page 456.

Modifying log handling settings on Linux computers

Each Virus and Spyware Protection policy includes log handling settings that apply to all virus and spyware scans that run on Linux client computers.

To log handling settings Linux computers

1 In the console, open a Virus and Spyware Protection policy.

2 Under **Linux Settings**, click **Miscellaneous**.

3 On the **Log Handling** tab, set options for event filtering, log retention, and log aggregation.

See "Viewing logs" on page 655.

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 466.

See "Managing Download Insight detections" on page 442.

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 the following options to use as additional criteria for examining unproven files:

- **Files with *x* or fewer users**
- **Files known by users for *x* or fewer days**

When unproven files meet these criteria, Download Insight detects the files as malicious.

5 Make sure that **Automatically trust any file downloaded from a trusted Internet or intranet site** 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, 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 and Linux clients, each detection category can be configured with a first action and a second action in case the first action is not possible.

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 or Linux clients

1. In the Virus and Spyware Protection policy, under **Windows Settings** or **Linux Settings**, 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: On Windows clients, 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 change the action that Symantec Endpoint Protection takes when it makes a detection on Mac clients

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**.

See "Customizing the virus and spyware scans that run on Windows computers" on page 466.

See "Customizing the virus and spyware scans that run on Mac computers" on page 467.

See "Customizing the virus and spyware scans that run on Linux computers" on page 468.

See "Managing Download Insight detections" on page 442.

See "Managing SONAR" on page 495.

See "Checking the scan action and rescanning the identified computers" on page 407.

See "Removing viruses and security risks" on page 404.

Allowing users to view scan progress and interact with scans on Windows computers

You can configure whether or not the scan progress dialog box appears on Windows 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.

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.

Note: Users can stop a Power Eraser analysis but cannot pause or snooze it.

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 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 **Advanced** tab, under **Scan Progress Options**, click **Show scan progress** or **Show scan progress if risk detected**.
4. To automatically close the scan progress indicator after the scan completes, check **Close the scan progress window when done**.
5. Check **Allow user to stop scan**.
6. Click **Pause Options**.
7. 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**.

8 Click **OK**.

See "Managing scans on client computers" on page 415.

Configuring Windows Security Center notifications to work with Symantec Endpoint Protection clients

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 3.

See "Customizing administrator-defined scans for clients that run on Windows computers" on page 473.

Note: You can configure all the Windows Security Center options on your client computers that run Windows XP SP3 only. You can only configure the **Display a Windows Security Center message when definitions are outdated** option or Windows Vista and Windows 7 and later.

Table 19-4 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.

Table 19-4 Options to configure how Windows Security Center works with the client *(continued)*

Option	Description	When to use
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.

To configure Windows Security Center to work with Symantec Endpoint Protection clients

1. In the console, open a Virus and Spyware Protection policy.
2. Under **Windows Settings**, click **Miscellaneous**.
3. On the **Miscellaneous** tab, specify options for the Windows Security Center.
4. Click **OK**.

Chapter 20

Managing the information that the management server and clients send to Symantec

This chapter includes the following topics:

Understanding server data collection and client submissions and their importance to the security of your network

By default, Symantec Endpoint Protection clients and Symantec Endpoint Protection Manager submit some types of pseudonymous information to Symantec. Clients can also send non-pseudonymous data to Symantec to get customized analysis. You can control whether or not your clients or Symantec Endpoint Protection Manager submit information.

Both server data and client submissions are critical to improving the security of your network.

What is server data collection?

Server data is part of the information that helps Symantec measure and improve the efficacy of detection technologies.

Symantec Endpoint Protection Manager submits the following types of pseudonymous information to Symantec:

- Licensing information, which includes the name, version, language, and licensing entitlement data
- Usage of Symantec Endpoint Protection protection features
- Information about Symantec Endpoint Protection configuration. The information includes operating system information, server hardware and software configuration, CPU size, memory size, and software version and features for installed packages

You can change the server submissions setting during installation, or change the setting on the server's **Site Properties > Data Collection** tab in the console.

Note: Symantec always recommends that you keep server data collection enabled.

What are pseudonymous client submissions?

Symantec Endpoint Protection clients automatically submit pseudonymous information about detections, network, and configuration to Symantec Security Response. Symantec uses this pseudonymous information to address new and changing threats as well as to improve product performance. Pseudonymous data is not directly identified with a particular user.

The detection information that clients send includes information about antivirus detections, intrusion prevention, SONAR, and file reputation detections.

Note: Mac client submissions do not include SONAR or file reputation submissions. Linux clients do not support any client submissions.

The pseudonymous information that clients send to Symantec benefits you by:

- Increasing the security of your network
- Optimizing product performance

In some cases, however, you might want to prevent your clients from submitting some information. For example, your corporate policies might prevent your client computers from sending any network information to outside entities. You can disable a single type of submission, such as submission of network information, rather than disabling all types of client submissions.

Note: Symantec recommends that you always keep client submissions enabled. Disabling submissions might interfere with faster resolution of false positive detections on the applications that are used exclusively in your organization. Without information about the malware in your organization, product response and Symantec response to threats might take longer.

See "Managing the pseudonymous or non-pseudonymous data that clients send to Symantec" on page 489.

See "How Symantec Endpoint Protection uses Symantec Insight to make decisions about files" on page 446.

See the section called "File reputation submissions" on page 447.

What are non-pseudonymous client submissions?

You can choose to submit non-pseudonymous client information to Symantec. This type of information provides insight into your security challenges that helps Symantec recommend customized solutions.

- You should use this option only if you participate in a Symantec-sponsored program that provides you custom analysis.
- The option is disabled by default.

See "Managing the pseudonymous or non-pseudonymous data that clients send to Symantec" on page 489.

Concerns about privacy

Symantec makes every attempt to pseudonymize the client submission data.

- Only suspicious executable files are submitted.
- User names are removed from path names.
- Computers and enterprises are identified by unique pseudonymized values.
- IP addresses are used for geographic location and then discarded.

For more information about privacy, see the following document:

Privacy statement

Concerns about bandwidth usage

Symantec Endpoint Protection minimizes the impact of client submissions on your network bandwidth.

You can check the Client Activity log to view the types of submissions that your client computers send and to monitor bandwidth usage.

See "How Symantec Endpoint Protection minimizes the impact of client submissions on your network bandwidth" on page 490.

See "Viewing logs" on page 655.

Managing the pseudonymous or non-pseudonymous data that clients send to Symantec

Symantec Endpoint Protection can protect computers by submitting pseudonymous information about detections to Symantec. Symantec 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.

See "Understanding server data collection and client submissions and their importance to the security of your network" on page 486.

Client computers submit information pseudonymously about detections. You can specify the types of detections for which clients submit information. The data that Symantec telemetry collects may include pseudonymous elements that are not directly identifiable. Symantec neither needs nor seeks to use telemetry data to identify any individual user.

Note: Mac client submissions do not include SONAR or file reputation submissions. Linux clients do not support any client submissions.

To change client submission settings

1. In the console, select **Clients** then click the **Policies** tab.
2. In the **Settings** pane, click **External Communications Settings**.
3. Select the **Client Submissions** tab.
4. Enable or disable the **Send pseudonymous data to Symantec to receive enhanced threat protection intelligence** option.
5. Select **More options** if you want to enable or disable specific submission types, such as file reputation.

6 If you participate in a Symantec-sponsored custom analysis program, select **Send client-identifiable data to Symantec for custom analysis**.

Warning: This option sends non-pseudonymous information to Symantec. Only use this option if you participate in a Symantec-sponsored program and want to share client-identifiable data with Symantec.

7 Select **OK**.

Note: On Mac clients, you can also disable IPS ping submissions. See the following article:

How to disable IPS data submission on Symantec Endpoint Protection for Mac clients

How Symantec Endpoint Protection minimizes the impact of client submissions on your network bandwidth

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.

See "Understanding server data collection and client submissions and their importance to the security of your network" on page 486.

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.

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.

To specify 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**.

For information about the recommended exceptions, see the following 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 "Understanding server data collection and client submissions and their importance to the security of your network" on page 486.

See "Creating exceptions for Virus and Spyware scans" on page 548.

Chapter 21

Managing SONAR and Tamper Protection

This chapter includes the following topics:

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, Memory Exploit Mitigation, 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.

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.

Note: SONAR does not inject code into applications on computers that run Symantec Endpoint Protection earlier than 12.1.2. If you use Symantec Endpoint Protection Manager 12.1.2 or later to manage clients, a SONAR file exception in an Exceptions policy is ignored on those 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.

See “Managing SONAR” on page 495.

See “Managing exceptions in Symantec Endpoint Protection” on page 544.

Managing SONAR

SONAR is part of Proactive Threat Protection on your client computers and the Virus and Spyware Protection policy in Symantec Endpoint Protection Manager.

Table 21-1 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 493.
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. See "Adjusting SONAR settings on your client computers" on page 498.
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 427.
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 "Understanding server data collection and client submissions and their importance to the security of your network" on page 486.
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 500. See "Monitoring endpoint protection" on page 625.

Table 21-1 Managing SONAR *(continued)*

Task	Description
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 498. See "Handling and preventing SONAR false positive detections" on page 497.
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 497.
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 Virus and Spyware scans" on page 548.
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 498. See "Creating an exception for an application that makes a DNS or host file change" on page 559.

Table 21-1 Managing SONAR *(continued)*

Task	Description
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 "Understanding server data collection and client submissions and their importance to the security of your network" on page 486.

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 "Understanding server data collection and client submissions and their importance to the security of your network" on page 486.

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.

Warning: If you set the action for high risk detections to log only, you might allow potential threats on your client computers.

Table 21-2 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 "Collecting information about the applications that the client computers run" on page 333. 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 498.
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" on page 561. See "Configuring how Windows clients handle quarantined items" on page 454. ■ 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 Virus and Spyware scans" on page 548.

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: A cloud icon appears next to some options when this domain is enrolled in the cloud console. If an Intensive Protection policy is in effect, the policy overrides these options for 14.0.1 clients only.

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.

   Note: When SONAR is enabled, Suspicious Behavior Detection automatically turns on. You cannot turn off Suspicious Behavior Detection when SONAR is enabled.

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.
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 559.
6. Under **Suspicious Behavior Detection**, you can change the action for high or low risk detections.

   If SONAR is disabled, you can also enable or disable Suspicious Behavior Detection.
7. Click **OK**.

See "Managing SONAR" on page 495.

See “Creating exceptions for Virus and Spyware scans” on page 548.

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 a SONAR 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.

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 **Additional 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" on page 561.

Changing Tamper Protection settings

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 client to block or log attempts to modify Symantec resources. You can create exceptions for the applications that Tamper Protection detects.

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 log actions.

5 Click **OK**.

See "Creating a Tamper Protection exception on Windows clients" on page 558.

Chapter 22

Managing application control, device control, and system lockdown

This chapter includes the following topics:

About application control, system lockdown, and device control

To monitor and control the behavior of applications on client computers, you use application control and system lockdown. Application control allows or blocks the defined applications that try to access system resources on a client computer. System lockdown allows only approved applications on client computers. To manage hardware devices that access client computers, you use device control.

Warning: Application control and system lockdown are advanced security features that only experienced administrators should configure.

You use application control, system lockdown, and device control for the following tasks.

Application control	■ 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. You configure application control and device control using an Application and Device Control policy. See "Setting up application control" on page 503.
System lockdown	■ 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. You configure system lockdown in the **Policies** tab on the **Clients** page. See "Configuring system lockdown" on page 516.
Device control	■ 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. See "Managing device control" on page 538.

Both application control and device control are supported on 32-bit and 64-bit Windows computers.

As of 14, Mac computers support device control.

Setting up application control

Application control allows or blocks the defined applications that try to access system resources on a client computer. You can allow or block access to certain registry keys, files, and folders. You can also define which applications are allowed to run, which applications that cannot be terminated through irregular processes, and which applications can call DLLs.

Use the following steps to set up application control on a group of client computers.

Table 22-1 Setting up application control

Steps	Description
Open a policy and enable default application control rule sets	Application Control policies contain predefined rule sets, which are disabled by default. You can enable any sets that you need, and apply the policy to a group. The predefined rule sets are configured in production mode rather than test mode. However, you should change the setting to test mode and test the rules in your test network before you apply them to your production network. See "Enabling and testing default application rules" on page 505.
Add additional application control rules (optional)	If the default rule sets do not meet your requirements, add new rule sets and rules. Typically, only advanced administrators should perform this task. See "Adding custom rules to Application Control" on page 507.
Add exceptions for applications	Application control injects code in some applications to examine them, which can slow applications that run on the computer. If necessary, you can exclude some applications from application control. You use an Exceptions policy to add file exceptions or folder exceptions for application control. See "Excluding a file or a folder from scans" on page 552.
View the Application Control logs	If you are testing a new policy or are troubleshooting an issue, you should monitor application control events in the log. In both test mode and production mode, application control events are in the Application Control log in Symantec Endpoint Protection Manager. On the client computer, application control and device control events appear in the Control log. 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. See "Viewing logs" on page 655.

Table 22-1 Setting up application control *(continued)*

Steps	Description
Prevent or allow users from enabling or disabling application control (optional)	In rare cases, application control might interfere with some safe applications that run on client computers. You might want to allow users to disable this option to troubleshoot problems. In the mixed mode or client mode, use the **Allow user to enable and disable the application device control** setting in the **Client User Interface Settings** dialog. See "Preventing users from disabling protection on client computers" on page 327.

You can also use system lockdown to allow approved applications or block unapproved applications on the client computers.

See "Configuring system lockdown" on page 516.

Enabling and testing default application rules

Application control includes default rule sets that are 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. To use the default rule sets in an Application Control policy, you must enable them and apply the policy to a group of clients.

For a description of the common predefined rules, see: Hardening Symantec Endpoint Protection (SEP) with an Application and Device Control Policy to increase security

In the following task you can enable and test the **Block writing to USB drives** rule set.

To enable a default application rule set

1. In the console, click **Policies** > **Application and Device Control**, and under **Tasks**, click **Add an Application Control Policy**.
2. In the **Overview** pane, type a name and description for the policy.
3. Click **Application Control**.
4. In the **Application Control** pane, check the **Enabled** check box next to each rule set that you want to implement.

   For example, next to the **Block writing to USB drives** rule set, check the check box in the Enabled column.
5. To review the rules for the rule set, select the rule, click **Edit**, and then click **OK**.

   See "Adding custom rules to Application Control" on page 507.
6. Change **Production** to **Test (log only)**.
7. Assign the policy to a group, and 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**.

   If application control is in effect, an **Unable to create folder** error message appears.

See "About application control, system lockdown, and device control" on page 502.

See "About the structure of an Application Control and Device Control policy" on page 506.

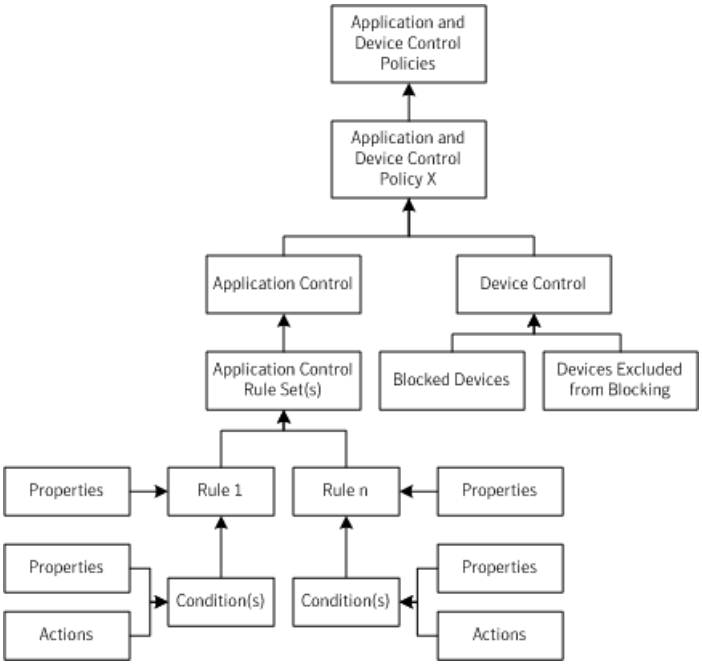
About the structure of an Application Control and Device Control policy

The Application and Device Control policy has two parts:

- Application Control contains one or more rule sets. Each rule set contains one or more rules. You configure properties, conditions, and actions for each rule:
  - **Rules** define the application(s) that you want to monitor.
  - **Conditions** monitor specified operations for the application(s) defined in the rule. The condition also contains the actions to take when the specified operation is observed.
  - As you add the rules and conditions, you need to specify the specific **properties** of the condition and what actions to take when the condition is met. Each condition type has different properties.
- 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



See "About application control, system lockdown, and device control" on page 502.

See "Setting up application control" on page 503.

See "Adding custom rules to Application Control" on page 507.

See "Managing device control" on page 538.

Adding custom rules to Application Control

If the default rule sets do not meet your requirements, add new rule sets and rules. You can also modify the predefined rule sets that are installed with the policy.

- The rule set is the container that holds one or more rules that allows or blocks an action.
- The rules in the rule sets define one or more processes or applications. You can also exclude a process from being monitored.
- Each rule includes the conditions and the actions that apply to a given process or processes. For each condition, you can configure actions to take when the condition is met. You configure rules to apply to only certain applications, and you can optionally configure them to exclude other applications from having the action applied.

See "About the structure of an Application Control and Device Control policy" on page 506.

Use the following steps to add your own application rules:

- Step 1: Add custom rule sets and rules
- Step 2: Define the application or process for the rule
- Step 3: Add conditions and actions to a rule
- Step 4: Test the rules before you apply them to your production network.
  See "Testing application control rules" on page 515.

Step 1: Add custom rule sets and rules

A best practice is to create a rule set that includes all of the actions that allow, block, and monitor a given task. On the other hand, you should create multiple rule sets if you have multiple tasks. For example, if you wanted to block write attempts to all removable drives and also block applications from tampering with a specific application, you should create two rules sets. You add and enable as many rule sets and rules as you need.

For example, BitTorrent is a communications protocol that is used for peer-to-peer file sharing and is not secure. BitTorrent distributes movies, games, music, and other files. BitTorrent is one of the simplest methods to distribute threats. Malware is hidden inside the files that are shared on peer-to-peer networks. You can use application control to block access to the BitTorrent protocol. You can also use peer-to-peer authentication and intrusion prevention.
See "Blocking a remote computer by configuring peer-to-peer authentication" on page 615.

Consider the order of the rules and their conditions when you configure them to avoid unexpected consequences. Typically, only advanced administrators should perform this task.

See "Best practices for adding application control rules" on page 511.

To add custom rule sets and rules

1. Open an Application Control policy.

   See "Enabling and testing default application rules" on page 505.

2. In the **Application Control** panel, under the list of default rule sets, click **Add**.

   To modify a predefined rule set, select it and then click **Edit**. For example, to monitor the applications that access the BitTorrent protocol, select **Block programs from running from removable drives [AC2]**.

3. In the **Add Application Control Rule Set** dialog box, type a name and description for the rule set.

4. Under Rules, select **Rule 1**, and on the **Properties** tab, type a meaningful name and description for the rule.

   To add an additional rule, click **Add** > **Add Rule**.

Step 2: Define the application or process for the rule

Each rule must have at least one application or process that it monitors on the client computer. You can also exclude certain applications from the rule. .

To define the application or process for the rule

1. With the rule selected, on the **Properties** tab, next to **Apply this rule to the following processes**, click **Add**.
2. In the **Add Process Definition** dialog box, type the application name or process name, such as `bittorrent.exe`.

   If you apply the rule to all applications except for a given set of applications, then define a wildcard for all (*) in this step. Then list the applications that need to be exceptions next to **Do not apply this rule to the following processes**.
3. Click **OK**.

The **Enable this rule** check box is enabled by default. If you uncheck this option, the rule does not apply.

Step 3: Add conditions and actions to a rule

The conditions control the behavior of the application or process that attempts to run on the client computer. Each condition type has its own properties to specify what the condition looks for.

Each condition has its own specific actions to take on the process when the condition is true. Except for the **Terminate process** action, the actions always apply to the process that you define for the *rule*, and not the *condition*.

Warning: The **Terminate process** action terminates the caller process, or the application that made the request. The caller process is the process that you define in the rule and not the condition. The other actions act on the target process, defined in the condition.

See "Best practices for choosing which condition to use for a rule" on page 513.

Condition	Description
Registry Access Attempts	Allows or blocks access to a client computer's registry settings.
File and Folder Access Attempts	Allows or blocks access to defined files or folders on a client computer.
Launch Process Attempts	Allows or blocks the ability to launch a process on a client computer.

Condition	Description
Terminate Process Attempts	Allows or blocks the ability to terminate a process on a client computer. For example, you may want to block a particular application from being stopped. **Warning:** The Terminate Process Attempt condition refers to the *target* process. If you use the **Terminate Process Attempts** condition on Symantec Endpoint Protection or another important process and then use the **Terminate process** action to kill the process that tries to kill Symantec Endpoint Protection.
Load DLL Attempts	Allows or blocks the ability to load a DLL on a client computer.

To add conditions and actions to a rule

1. Under **Rules**, select the rule you added, click **Add** > **Add Condition**, and choose a condition.

   See "Best practices for choosing which condition to use for a rule" on page 513.

   For example, click **Launch Process Attempts** to add a condition for when the client computer accesses the BitTorrent protocol.

2. On the **Properties** tab, select the process that should or should not be launched:

   - To specify a process to launch:
     Next to **Apply to the following *entity***, click **Add**.
   - To exclude a process from being launched:
     Next to **Do not apply to the following processes**, click **Add**.

3. In the **Add *entity* Definition** dialog box, type process name, DLL, or registry key.

   For example, to add BitTorrent, type its file path and executable, such as:
   `C:\Users\UserName\AppData\Roaming\BitTorrent`

   To apply a condition to all processes 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.

4. Click **OK**.

5. On the **Actions** tab for the condition, select an action to take.

   For example, to block Textpad if it tries to launch Firefox, click **Block access**.

6 Check **Enable logging** and **Notify user**, and add a message you want the client computer user to see.

For example, type **Textpad tries to launch Firefox**.

7 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.

Best practices for adding application control rules

You should plan your custom application control rules carefully. When you add application control rules, keep in mind the following best practices.

Table 22-2 Best practices for application control rules

Best practice	Description	Example
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 22-2 Best practices for application control rules *(continued)*

Best practice	Description	Example
Use the right action	The **Terminate Process Attempts** condition allows or blocks an application's ability to terminate the calling 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.
Use one rule set per goal	Create one rule set that includes all of the actions that allow, block, or monitor a 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 instead of one rule set.
Use the **Terminate process** action sparingly	The **Terminate process** action kills the calling 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. Instead, use the **Block access** action, which blocks the target process, or Winword.exe.

Table 22-2 Best practices for application control rules *(continued)*

Best practice	Description	Example
Test rules before you put them into production	The **Test (log only)** option for rule sets logs the actions, and does not apply to the actions to the client computer. Run rules in test mode for some acceptable period of time before you switch them back to production mode. During this time period, review the Application Control logs and verify that the rules work as planned.	The test option reduces potential accidents you might make by not considering all possibilities of the rule. See "Testing application control rules" on page 515.

See "Adding custom rules to Application Control" on page 507.

See "Best practices for choosing which condition to use for a rule" on page 513.

Best practices for choosing which condition to use for a rule

You add custom application control rules and conditions to prevent users from opening applications, writing to files, or sharing files. 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 "Adding custom rules to Application Control" on page 507.

Table 22-3 Typical conditions to use for a rule

Rule	Condition
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 for this type of rule.

Table 22-3 Typical conditions to use for a rule *(continued)*

Rule	Condition
Block file shares on Windows computers	You can 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**. 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 367.
Prevent users from running peer-to-peer applications	You can 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**. 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 page 377. See "Creating a firewall policy" on page 340.
Block write attempts to DVD drives	Currently, application control does not have a default rule that blocks CD/DVD writing directly. Instead, you create a rule that blocks the specific DLLs that write to CD or DVD drives using the **Add Condition** and **File and Folder Access Attempts** conditions. You should also create a Host Integrity policy that sets the Windows registry key to block write attempts to DVD drives. See "Setting up Host Integrity" on page 606. See: How to block CD/DVD Writing in Windows 7

Testing application control rules

After you add application control rules, you should test them in your network. Configuration errors in the rule sets that are used in an Application 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. After you test the rules, apply them to your production network.

Step 1: Set the rule set to test mode

You test rule sets by setting the mode to test mode. Test mode creates a log entry to indicate when rules in the rule set would be applied without actually applying the rule.

Default rules use production mode by default. Custom rules use test mode by default. You should test both default and custom 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.

Changing a rule set to test mode

1. In the console, open an Application and Device Control policy.
2. Under **Application Control Policy**, click **Application Control**.
3. In the **Application Control Rule Sets** list, click the drop-down arrow in the **Test/Production** column for the rule set, and click **Test (log only)**.

See "Setting up application control" on page 503.

Step 2: Apply the Application and Device Control policy to computers in your test network

If you created a new Application and Device Control policy, apply the policy to clients in your test network.

See "Assigning a policy to a group or location" on page 321.

Step 3: Monitor the Application Control log

After you run your rule sets in test mode for a period of time, check the logs for any errors. In both test mode and production mode, application control events are in the Application Control log in Symantec Endpoint Protection Manager. On the client computer, application control and device control events appear in the Control log.

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.

See "Viewing logs" on page 655.

Step 4: Change the rule set back to production mode

When the rules function like you expect them to, change the rule set back 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 includes 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 22-4 System lockdown steps

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. When you run system lockdown, you need a file fingerprint list that includes all of the applications you want to whitelist or blacklist. 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 create a file fingerprint list in the following ways: ■ 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. Use the utility to create a checksum for a particular application or all the applications in a specified path. Use this method to generate file fingerprints to use when you run system lockdown in blacklist mode. See "Creating a file fingerprint list with checksum.exe" on page 522. ■ Create a file fingerprint list on a single computer or small group of computers using the Collect File Fingerprint List command. In 12.1.6 or later, you can run the Collect File Fingerprint List command from the console. The command collects a file fingerprint list that includes every application on the targeted computers. For example, you might run the command on a computer that runs a gold image. You can use this method when you run system lockdown in whitelist mode. Note that the file fingerprint list that you generate with the command cannot be modified. When you re-run the command, the file fingerprint list is automatically updated. See "Running commands on client computers from the console" on page 253. ■ Create a file fingerprint list with any third-party checksum utility. **Note:** In 12.1.6 or later, if you run Symantec EDR in your network, you might see file fingerprint lists from Symantec EDR. See "Interaction between system lockdown and Symantec EDR blacklist rules" on page 526.

Table 22-4 System lockdown steps *(continued)*

Action	Description
Step 2: Import file fingerprint lists into Symantec Endpoint Protection Manager	Before you can use a file fingerprint list in the system lockdown configuration, the list must be available in Symantec Endpoint Protection Manager. When you create file fingerprint lists with a checksum tool, you must manually import the lists into Symantec Endpoint Protection Manager. See "Importing or merging file fingerprint lists in Symantec Endpoint Protection Manager" on page 524. When you create a file fingerprint list with the Collect File Fingerprint List command, the resulting list is automatically available in the Symantec Endpoint Protection Manager console. 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. You can also manually enter individual application names in the system lockdown configuration. **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 527.

Table 22-4 System lockdown steps *(continued)*

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. 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 532.
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 532.

Table 22-4 System lockdown steps *(continued)*

Action	Description
Step 6: Enable system lockdown	By default, system lockdown runs in whitelist mode. You can configure system lockdown to run in blacklist mode instead. When you enable system lockdown in 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 "Running system lockdown in whitelist mode" on page 534. See "Running system lockdown in blacklist mode" on page 535.

Table 22-4 System lockdown steps *(continued)*

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 the following ways: ■ Manually append, replace, or merge file fingerprint lists that you imported. You cannot append file fingerprint lists to a fingerprint list that you generate with the Collect File Fingerprint List command. You can append an imported list with a command-generated list. In that case, if you re-run the fingerprint command, you must recreate the appended list. See "Manually updating a file fingerprint list in Symantec Endpoint Protection Manager" on page 525. See "Importing or merging file fingerprint lists in Symantec Endpoint Protection Manager" on page 524. ■ Automatically update existing file fingerprint lists that you imported. You can also automatically update applications or the application name lists that you import. See "Automatically updating whitelists or blacklists for system lockdown" on page 528. See "Creating an application name list to import into the system lockdown configuration" on page 527. ■ Re-run the Collect File Fingerprint List command to automatically update a command-generated fingerprint list. When you re-run the command, the new list automatically replaces the existing list. **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 and disable system lockdown. Or you can keep system lockdown enabled and run the configuration in log-only mode. You can also 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 532.

Table 22-4 System lockdown steps *(continued)*

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** 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. See "Testing selected items before you add or remove them when system lockdown is already enabled" on page 537.

See "Setting up application control" on page 503.

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 following for each executable file or DLL that resides in a specified path on the computer:

- The path
- The file name
- The corresponding checksum

You then import the file fingerprint list into Symantec Endpoint Protection Manager to use in your system lockdown configuration.

The utility is installed with Symantec Endpoint Protection on the client computer.

See "Importing or merging file fingerprint lists in Symantec Endpoint Protection Manager" on page 524.

See "Configuring system lockdown" on page 516.

You can also use a third-party utility or the Collect File Fingerprint List command to create a file fingerprint list.

See "Running commands on client computers from the console" on page 253.

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 client installation folder, which contains the file checksum.exe. Typically, the file is located in the following folder:

   C:\Program Files (x86)\Symantec\Symantec Endpoint Protection\

3. Type the following command:

   `checksum.exe` *`outputfile.txt`* *`path`*

   Where:

   - *outputfile.txt* is the name of the resulting text file that contains the checksums for all the applications that are located on the specified drive.
   - *path* is the file path on the computer on which you want to gather checksum information.

   Note: To run a checksum against all files on the C drive, you must add a forward slash at the end of *path*. Otherwise, the command only runs in the folder where `checksum.exe` is located.

   The format of each line in the output file is as follows:

   checksum_of_the_file full_pathname_of_the_exe_or_DLL

   A space separates the checksum value and the full pathname.

   An example of checksum.exe output is shown here:

```
0bb018fad1b244b6020a40d7c4eb58b7 c:\dell\openmanage\remind.exe
35162d98c2b445199fef95e838feae4b c:\dell\pnp\m\co\HSFCI008.dll
2f276c59243d3c051547888727d8cc78 c:\Nokia Video Manager\QtCore4.dll
```

Example syntax

The following is an example of the syntax you can use to create a fingerprint list for all of the files on the C drive:

```
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 computer on which it runs.

The following is an example of the syntax that you can 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

File fingerprint lists must be available in the Symantec Endpoint Protection Manager console so that you can add them to the system lockdown configuration. When you create file fingerprint lists with the checksum.exe utility or a third-party checksum tool, you must manually import the lists. You can also merge file fingerprint lists.

File fingerprint lists that you create with the Collect File Fingerprint List command are automatically available in the console. You do not need to import them. You cannot modify file fingerprint lists that you created with the Collect File Fingerprint List command. You can, however, merge a command-generated file fingerprint list with another file fingerprint list. If you run the command again to re-generate the list, you must manually merge the lists again.

See "Configuring system lockdown" on page 516.

See "Creating a file fingerprint list with checksum.exe" on page 522.

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 on the **Policies** tab under **Policies > Policy Components > 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 that you imported. You cannot directly edit any existing file fingerprint list in Symantec Endpoint Protection Manager.

If you want to merge fingerprint lists into a new list with a different name, use the **Add a File Fingerprint Wizard**.

If you create a fingerprint list with the Collect File Fingerprint List command, you cannot append, replace, or remove the entries. You can, however, append a command-generated list to an imported list. If you re-run the command, you must manually update the fingerprint list again.

You cannot modify any file fingerprint list that Symantec EDR sends to Symantec Endpoint Protection Manager.

See "Importing or merging file fingerprint lists in Symantec Endpoint Protection Manager" on page 524.

See "Configuring system lockdown" on page 516.

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 one**.
- Click **Remove any fingerprints that also appear on 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** > **Close** > **Finish**.

Interaction between system lockdown and Symantec EDR blacklist rules

If your network includes Symantec EDR, you might see blacklists in the system lockdown configuration from Symantec EDR.

Symantec EDR blacklists interact with the system lockdown configuration in the following ways:

- When Symantec Endpoint Protection Manager receives a blacklist rule from Symantec EDR, Symantec Endpoint Protection Manager enables system lockdown in blacklist mode for all domains and groups.
- The blacklist rule appears in the Symantec Endpoint Protection Manager file fingerprint list in the system lockdown configuration. You cannot modify a file fingerprint list from Symantec EDR.
- If you configured a client group with system lockdown enabled in whitelist mode, the setting is preserved and Symantec Endpoint Protection Manager does not use the Symantec EDR blacklist rule.
- If you disable system lockdown and delete the Symantec EDR blacklist, Symantec Endpoint Protection Manager automatically re-enables system lockdown and applies the blacklist.
- If you disable system lockdown but do not delete the Symantec EDR blacklist, system lockdown remains disabled until you re-enable it.

Note: Symantec EDR sends whitelist rules directly to Symantec Endpoint Protection clients. Symantec EDR does not send whitelist file fingerprints to Symantec Endpoint Protection Manager.

See "Running system lockdown in whitelist mode" on page 534.

See "Running system lockdown in blacklist mode" on page 535.

See "Configuring client groups to use private servers for reputation queries and submissions" on page 463.

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. 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 22-5 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 "Configuring system lockdown" on page 516.

Automatically updating whitelists or blacklists for system lockdown

Symantec Endpoint Protection Manager can automatically update existing file fingerprint lists and application name lists that you imported, merged, or appended.

File fingerprint lists that you generate from the Collect File Fingerprint List command are automatically updated when you re-run the command on the same computer.

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 22-6 Updating whitelists or blacklists for system lockdown

Step	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 522. A fingerprint list that you generate from the Collect File Fingerprint List command cannot be updated directly. You can merge a command-generated list with another list, or append an imported list with a command-generated list. 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.

Table 22-6 Updating whitelists or blacklists for system lockdown *(continued)*

Step	Description
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 530.
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. For UNC, only JCFIS shares are supported. DFS shares are not supported. **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: C:\Program Files (x86)\Symantec\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 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. See "Enabling automatic updates of whitelists and blacklists for system lockdown" on page 531.
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 532.

See "Manually updating a file fingerprint list in Symantec Endpoint Protection Manager" on page 525.

See "Configuring system lockdown" on page 516.

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 528.

See "Creating an application name list to import into the system lockdown configuration" on page 527.

Enabling automatic updates of whitelists and blacklists for system lockdown

You can configure Symantec Endpoint Protection Manager to automatically update whitelists and blacklists that you use for system lockdown.

To automatically update a file fingerprint list that you generated with the Collect File Fingerprint List command, run the command again.

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.
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**.

See "Automatically updating whitelists or blacklists for system lockdown" on page 528.

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 528.

See "Viewing logs" on page 655.

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. Click **Log Unapproved Applications Only** to run system lockdown in test mode.

   This option logs the unapproved applications that clients are currently running.
4. Select **Whitelist Mode** or **Blacklist Mode**.

5 Under **Application File Lists**, under **File Fingerprint List**, add or remove file fingerprint lists.

To add a list, the list must available in Symantec Endpoint Protection Manager.

See "Importing or merging file fingerprint lists in Symantec Endpoint Protection Manager" on page 524.

6 To add an application name list, under **Application File Lists**, under **File Name**, click **Import**.

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 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 527.

7 To add an individual application, under **Application File Lists**, under **File Name**, click **Add**.

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 516.

Running system lockdown in whitelist mode

You can configure 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 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.

Warning: 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.

See "Setting up and testing the system lockdown configuration before you enable system lockdown" on page 532.

Note: If you run system lockdown enabled in whitelist mode, Symantec Endpoint Protection Manager does not apply any blacklist rules from Symantec EDR.

See "Interaction between system lockdown and Symantec EDR blacklist rules" on page 526.

Running system lockdown 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. Under **System Lockdown**, select **Enable System Lockdown** to block any unapproved applications that clients try to run.
5. Under **Application File Lists**, select **Whitelist Mode**.
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 "Configuring system lockdown" on page 516.

See "Disabling a group's inheritance" on page 242.

Running system lockdown 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: If you run Symantec EDR in your network, the Symantec EDR configuration affects the system lockdown blacklist configuration.

See "Interaction between system lockdown and Symantec EDR blacklist rules" on page 526.

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.

See "Setting up and testing the system lockdown configuration before you enable system lockdown" on page 532.

Warning: 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.

Running system lockdown 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 a group's inheritance" on page 242.
3. On the **Policies** tab, select **System Lockdown**.
4. Under **System Lockdown** dialog box, select **Enable System Lockdown**.
5. Under **Application File Lists**, select **Blacklist Mode**.
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 "Setting up and testing the system lockdown configuration before you enable system lockdown" on page 532.

See "Configuring system lockdown" on page 516.

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.

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 “Running system lockdown in whitelist mode” on page 534.

   See “Running system lockdown in blacklist mode” on page 535.

4 In whitelist mode, under **Application File Lists**, check **Test Before Removal** next to an existing 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** 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 532.

See "Configuring system lockdown" on page 516.

Managing device control

Device control specifies what hardware devices are allowed or blocked on your client computers. You use the default hardware devices list and a Device Control policy to manage device control. You can also add your own.

Table 22-7 Managing device control

Step	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 541.
Add devices to the hardware device list (if necessary)	When you add a device to the device list, you need a class ID or device ID for the device. You cannot add a customized device for Mac. You can only use the device types that are provided. See "Adding a hardware device to the Hardware Devices list" on page 542. See "Obtaining a device vendor or model for Windows computers with DevViewer" on page 541.
Allow or block a device in the Device Control policy	Specify the devices that you want to allow or block from being accessed on the client. See "Allowing or blocking devices on client computers" on page 539.

For Mac clients, device control is part of SymDaemon service. You do not need to restart the Windows client or the Mac client for device control to work.

See "About application control, system lockdown, and device control" on page 502.

See the section called "**Device Control** differences based on platform" on page 808.

Allowing or blocking devices on client computers

You use an Application and Device Control policy to configure device control. Before you begin, add any devices you need to the **Hardware Devices** list.

See "Adding a hardware device to the Hardware Devices list" on page 542.

As of 14, you can configure both Windows and Mac device control.

To configure device control for Windows clients

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 specific ports, then 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 **OK**.

To configure device control for Mac clients (as of 14)

1 In the console, open an Application and Device Control policy.

2 Under **Mac Settings**, click **Device Control**.

3 Under **Blocked Devices**, click **Add**.

4 In the **Device Selection** window, select a device from the list. You can only add one device at a time.

Fill in the fields at the bottom of the window, if available. If you leave the fields blank, all devices of this type are blocked.

You can also use regular expressions to define device vendor, device model, or serial number. See the Help in the **Mac Device Control** window for more information.

To obtain the serial number, model number, or vendor name from a Mac-connected device, use the DeviceInfo tool from the installation file. You can find this tool and its instructions under `Tools/DeviceInfo`.

5 Click **OK**.

6 Under **Devices Excluded From Blocking**, click **Add**.

7 In the **Device Selection** window, select a device from the list, define the excluded devices, and then click **OK**.

8 Check **Notify users when devices are blocked** if you want to notify the user.

9 Click **OK**.

See “Managing device control” on page 538.

See “About application control, system lockdown, and device control” on page 502.

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 538.

You can add devices to the list. You cannot edit or delete any default devices.

You cannot add a customized hardware device for Mac.

Devices are identified by a device ID or class ID. You use either of these values to add a device to the list. You can use a tool to determine the device ID or the class ID. For Windows, go to Tools\DevViewer. For the Mac, go to Tools\DeviceInfo.

See "Obtaining a device vendor or model for Windows computers with DevViewer" on page 541.

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 device vendor or model for Windows computers with DevViewer

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. In the full product installation file from MySymantec, locate the `Tools\DevViewer` folder, and then copy the `DevViewer.exe` tool to the client computer.

   See Getting Started with MySymantec.

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 **Disk 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 542.

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 541.

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. You may need to replace the curly braces with the wildcard character `?`.

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 device vendor or model for Windows computers with DevViewer" on page 541.

7 Click **OK**.

Chapter 23

Managing exceptions

This chapter includes the following topics:

Managing exceptions in Symantec Endpoint Protection

You can manage exceptions for Symantec Endpoint Protection in the Symantec Endpoint Protection Manager console.

Table 23-1 Managing exceptions

Task	Description
Learn about exceptions	You use exceptions to exclude items from being scanned on your client computers. See "About exceptions in scans based on the operating system" on page 547.

Table 23-1 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 424.
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 Virus and Spyware scans" on page 548. See "Creating exceptions from log events" on page 561.
Restricting the types of exceptions that users can configure on client computers (Windows only)	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 561.
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" on page 561.
Create exceptions for intrusion prevention signatures	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 "Creating exceptions for IPS signatures" on page 384.

Which Windows exceptions do I use for what type of scan?

Table 23-2 lists which exception types are used in the Exceptions policy for which types of scans in Version 14 MPx and earlier.

Table 23-2 Exception names for version 14.0.1 and earlier

Symantec Endpoint Protection Manager 14.0.1 and earlier	Client restrictions (on Symantec Endpoint Protection Manager)*	Windows client	What is exception used for?
Application	Application Exception	Application Exception	■ Auto-Protect ■ Manual scans ■ Scheduled scans ■ Download Insight ■ SONAR
Application to Monitor	Not available	Not available	Application Control
Certificate	Not available	Not available	■ Auto-Protect ■ Manual scans ■ Scheduled scans ■ Download Insight ■ SONAR
DNS or Host File Change	DNS or Host File Change Exception	DNS or Host File Change Exception > Application	SONAR
Extensions	Extensions Exception	Security Risk Exception > Extensions	■ Auto-Protect ■ Manual scans ■ Scheduled scans
File	File Exception	Security Risk Exception > File	■ Auto-Protect ■ Manual scans ■ Scheduled scans ■ SONAR ■ Application Control
Folder	Folder Exception: ■ Security risk Exception ■ SONAR Exception	Security Risk Exception > Folder SONAR Exception	■ Auto-Protect ■ Manual scans ■ Scheduled scans ■ SONAR ■ Application Control

Table 23-2 Exception names for version 14.0.1 and earlier *(continued)*

Symantec Endpoint Protection Manager 14.0.1 and earlier	Client restrictions (on Symantec Endpoint Protection Manager)*	Windows client	What is exception used for?
Known Risks	Known risks Exception	Security Risk Exception > Known Risks	■ Auto-Protect ■ Manual scans ■ Scheduled scans ■ SONAR
Trusted Web Domain	Trusted web domain Exception	Security Risk Exception > Web Domain	Download Insight
Tamper Protection Exception	Not available	Not available	Applications that Tamper Protection protects

*Client restrictions are the exceptions that you can display or hide on the client for the client user to add. Exceptions that you add in the cloud console are unavailable in Symantec Endpoint Protection Manager to enable or disable on the client.

See "Restricting the types of exceptions that users can configure on client computers" on page 561.

See "How does the Symantec Endpoint Protection Manager Exceptions policy interact with the cloud console?" on page 595.

About exceptions in scans based on the operating system

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 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.

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.

Note: You cannot create exceptions for an individual virus and spyware scan. 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, Mac, or Linux). You configure the exceptions for each client type separately.

Table 23-3 Operating system type and scan exceptions

Client Type	Exception
Windows clients	■ File ■ Folder ■ Known risk ■ Extension ■ Trusted Web domain ■ Application to monitor ■ Application ■ Tamper Protection
Mac clients	■ File or folder exception
Linux clients	■ Folder or extension exception

See "About the files and folders that Symantec Endpoint Protection excludes from virus and spyware scans" on page 424.

See "Managing exceptions in Symantec Endpoint Protection" on page 544.

Creating exceptions for Virus and Spyware scans

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.

Exceptions for virus and spyware scans also apply to Download Insight.

Table 23-4 Creating exceptions for Symantec Endpoint Protection

Task	Description
Exclude a file from virus and spyware scans	Supported on Windows and Mac clients. Excludes a file by name from virus and spyware scans, SONAR, or application control on Windows clients. See "Excluding a file or a folder from scans" on page 552.
Exclude a folder from virus and spyware scans	Supported on Windows, Mac, and Linux clients. Excludes a folder from virus and spyware scans, SONAR, or all scans on Windows clients. On Windows and Linux clients, you can choose to limit an exception for virus and spyware scans to Auto-Protect or scheduled and on-demand scans only. If you run an application that writes many temp files to a folder, you might want to exclude the folder from Auto-Protect. Auto-Protect scans files as they are written so you can increase computer performance by limiting the exception to scheduled and on-demand scans. You might want to exclude the folders that are not often used or that contain archived or packed files from scheduled and on-demand scans. For example, scheduled or on-demand scans of deeply archived files that are not often used might decrease computer performance. Auto-Protect still protects the folder by scanning only when any files are accessed or written to the folder. See "Excluding a file or a folder from scans" on page 552.
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. Security risk exceptions do not apply to SONAR. See "Excluding known risks from virus and spyware scans on Windows clients" on page 555.
Exclude file extensions from virus and spyware scans	Supported on Windows and Linux clients. Excludes any files with the specified extensions from virus and spyware scans. Extension exceptions do not apply to SONAR or to Power Eraser. See "Excluding file extensions from virus and spyware scans on Windows clients and Linux clients" on page 555.

Table 23-4 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 Windows clients" on page 556.
Specify how virus and spyware 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. 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 Windows clients" on page 556. See "Collecting information about the applications that the client computers run" on page 333.

Table 23-4 Creating exceptions for Symantec Endpoint Protection *(continued)*

Task	Description
Exclude a web domain from virus and spyware scans	Supported on Windows clients. Download Insight scans the files that users try to download from websites 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 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 Windows clients" on page 557.
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 Windows clients" on page 558.

Table 23-4 Creating exceptions for Symantec Endpoint Protection *(continued)*

Task	Description
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 559.
Exclude a certificate	Supported on Windows clients (starting in 14.0.1). You can exclude a certificate from scans. Excluding a certificate prevents it from being flagged as suspicious. A Download Insight scan can flag a self-signed certificate on an internal tool as suspicious, for example. See "Excluding a certificate from scans on Windows clients" on page 560.

See "Managing exceptions in Symantec Endpoint Protection" on page 544.

See "Creating exceptions from log events" on page 561.

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**.

See the help for information about why you might want to limit the exception to a specific type of security risk scan.

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**.

See the help for information about why you might want to limit the exception to a specific type of security risk scan.

7 Click **OK**.

To exclude a file or folder from scans 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 file or 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**.

To exclude a folder from scans on Linux clients

1 On the **Exceptions Policy** page, click **Exceptions**.

2 Under **Exceptions**, click **Add > Linux Exceptions**.

3 Click **Folder**.

4 In the **Add Folder Exception** dialog box, you can choose a prefix variable, type a folder name, and either include subfolders or not.

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 Specify the type of security risk scan. Select **Auto-Protect**, **Scheduled and on-demand**, or **All scans**, and then click **OK**.

See "Creating exceptions for Virus and Spyware scans" on page 548.

See "Excluding file extensions from virus and spyware scans on Windows clients and Linux clients" on page 555.

Excluding known risks from virus and spyware scans on Windows clients

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.

To exclude known risks from virus and spyware scans on Windows clients

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**.

See "Creating exceptions for Virus and Spyware scans" on page 548.

Excluding file extensions from virus and spyware scans on Windows clients and Linux clients

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 Virus and Spyware scans" on page 548.

To exclude file extensions from virus and spyware scans on Windows clients and Linux clients

1. On the **Exceptions Policy** page, click **Exceptions**.
2. Under **Exceptions**, click **Add > Windows Exceptions > Extensions** or **Add > Linux Exceptions > Extensions**.
3. In the text box, type the extension that you want to exclude, and then click **Add**.

4 Under **Specify the type of security risk scan**, select **Auto-Protect**, **Scheduled and on-demand**, or **All Scans**.

5 Add any other extensions to the exception.

6 Click **OK**.

See "Excluding a file or a folder from scans" on page 552.

Monitoring an application to create an exception for the application on Windows clients

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.

To monitor an application to create an exception for the application on Windows clients

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 Click **OK**.

See "Monitoring the applications and services that run on client computers" on page 331.

See "Creating exceptions for Virus and Spyware scans" on page 548.

See "Specifying how Symantec Endpoint Protection handles monitored applications on Windows clients" on page 556.

See "Creating exceptions from log events" on page 561.

Specifying how Symantec Endpoint Protection handles monitored applications on Windows clients

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**.

To specify how Symantec Endpoint Protection handles monitored applications on Windows clients

1. On the **Exceptions Policy** page, click **Exceptions**.
2. Click **Add > Windows Exceptions > Application**.
3. In the **View** drop-down box, 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 as bad or malicious. The **Terminate**, **Quarantine**, and **Remove** actions apply when the application launches.
6. Click **OK**.

See "Monitoring an application to create an exception for the application on Windows clients" on page 556.

See "Creating exceptions for Virus and Spyware scans" on page 548.

See "Monitoring the applications and services that run on client computers" on page 331.

See "Creating an exception for an application that makes a DNS or host file change" on page 559.

Excluding a trusted web domain from scans on Windows clients

You can exclude a web domain from virus and spyware scans and from SONAR. When you exclude a trusted web domain, any file that the user downloads from any location within that domain is always allowed. However, Auto-Protect and other defined scans still scan the file.

By default, Download Insight excludes the websites that appear on the **Internet Trusted Sites** list through **Internet Explorer > Tools > Internet Options > Security**. You can configure this setting from the Download Insight settings in the **Virus and Spyware Protection** policy.

If Download Insight or Auto-Protect is disabled, trusted web domain exceptions are also disabled.

Note: You should use caution when you configure exceptions. Every exception that you create lowers the security profile of the computer. Consider submitting any suspected false positives for examination rather than opening a permanent scan exclusion. Always use the multiple layers of protection that Symantec Endpoint Protection provides.

Report a Suspected Erroneous Detection (False Positive)

Supported web domain exceptions

Follow these guidelines when you create a web domain exception:

- You must enter a single domain as a URL or an IP address when you specify a trusted web domain exception. You can specify only one domain at a time.
- Port numbers are not supported.
- When you specify a URL, the exception uses only the domain name portion of a URL. You can prepend the URL with either HTTP or HTTPS (case-insensitive), but the exception applies to both protocols.
- When you specify an IP address, the exception applies to both the specified IP address and its corresponding host name. If a user navigates to a location through its URL, Symantec Endpoint Protection resolves the host name to the IP address and applies the exception. You can prepend the IP address only with HTTP (case-insensitive).
- Both Download Insight and SONAR exclude the domain regardless of whether a user navigates to the domain through HTTP or HTTPS.
- For an FTP location, you must specify an IP address. FTP URLs are not supported.
- The wildcard * is supported for use with exceptions for trusted web domains.

To exclude a trusted web domain from scans on Windows clients

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 domain name or IP address that you want to exclude.

   See the section called “Supported web domain exceptions” on page 558.
3. Click **OK**.
4. Repeat the procedure to add more web domain exceptions.

See “Creating exceptions for Virus and Spyware scans” on page 548.

Creating a Tamper Protection exception on Windows clients

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.

To create Tamper Protection exception on Windows clients

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**.

See How to collect the Tamper Protection log from Symantec Endpoint Protection Manager in Symantec Endpoint Protection 12.1.

See “Creating exceptions for Virus and Spyware scans” on page 548.

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 Virus and Spyware scans" on page 548.

See "Specifying how Symantec Endpoint Protection handles monitored applications on Windows clients" on page 556.

See "Adjusting SONAR settings on your client computers" on page 498.

Excluding a certificate from scans on Windows clients

As of 14.0.1, you can add exceptions for certificates individually to prevent the files that it signs from being scanned and detected as suspicious. For example, a tool that your company developed internally may use a self-signed certificate. Excluding this certificate from scans prevents Auto-Protect, Download Insight, SONAR, or other scans from detecting the files that it signs as suspicious.

The certificate exclusion supports the X.509 and base64 certificate types only. When you add a certificate exception, you need a copy of the public certificate in a DER or base64 encoded file (.cer).

Certificate exclusions are not supported for the following items:

- Memory Exploit Mitigation
- Proactive Threat Protection system change events
- Tamper Protection
- Certificate-signed files within a compressed file

The excluded certificate does not have to be installed in the certificate store on the client computer in order for the exclusion to work. In the case of a conflict between a certificate exception and a blacklist rule, the blacklist rule takes precedence.

You can only add a certificate exception through the Symantec Endpoint Protection Manager policy, not through the Symantec Endpoint Protection client interface settings.

Note: You can only add a certificate exception in Symantec Endpoint Protection Manager if it is unenrolled from the cloud console. If Symantec Endpoint Protection Manager is enrolled, use the cloud console to add or manage a certificate exception.

To exclude a certificate from scans on Windows clients

1. On the **Exceptions Policy** page, click **Exceptions**.
2. Under **Exceptions**, click **Add > Windows Exceptions > Certificate**.

   If Symantec Endpoint Protection Manager is enrolled in the cloud console, this option does not appear. Instead, add certificate exceptions in the cloud console.
3. Under **Certificate File**, click **Browse** to navigate to the certificate that you want to exclude, and then click **OK**.
4. Confirm that the values under **Certificate Information** are correct for the certificate that you want to exclude, and then click **OK**.

   To create exceptions for more than one certificate, repeat the procedure.

See "Creating exceptions for Virus and Spyware scans" on page 548.

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.

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**.

See "Managing exceptions in Symantec Endpoint Protection" on page 544.

Creating exceptions from log events

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 23-5 Exceptions and log types

Exception Type	Log Type
File	Risk log
Folder	Risk log SONAR log
Known risk	Risk log
Extension	Risk log
Application	Risk log SONAR log
Trusted Web domain	Risk log SONAR log
Tamper Protection	Application Control log
DNS or host file change	SONAR log

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.

To create exceptions from log events

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**.

See “Monitoring endpoint protection” on page 625.

See “Managing exceptions in Symantec Endpoint Protection” on page 544.

See “Creating exceptions for Virus and Spyware scans” on page 548.

Chapter 24

Managing integrations

This chapter includes the following topics:

Managing integrations in Symantec Endpoint Protection

The Integrations policy in Symantec Endpoint Protection Manager lets you manage integrations with other Symantec products that you use in your environment.

Table 24-1 Managing integrations

Integration	Description
Web Security Services (WSS) Traffic Redirection	WSS Traffic Redirection (WTR) integrates Symantec Web Security Service functionality into Symantec Endpoint Protection. You can specify the URL for a proxy auto-configuration (PAC) file that you configure in Symantec Web Security Services. You can also enable a local proxy service for further granular control over web traffic redirection. See "Configuring WSS Traffic Redirection" on page 564.

Configuring WSS Traffic Redirection

Web Security Service (WSS) Traffic Redirection (WTR) integrates Symantec Web Security Service functionality into Symantec Endpoint Protection as of version 14.0.1 MP1. Symantec Web Security Service provides broad connectivity options to securely redirect web traffic, whether the user is on-premises or off of the corporate network. Symantec Web Security Service offers several access methods. For more information, see:

Web Security Service Access Method

By adding WSS Traffic Redirection to Symantec Endpoint Protection, you can automate web traffic redirection to Symantec Web Security Service and secure the web traffic on each endpoint that uses Symantec Endpoint Protection.

To use this feature within Symantec Endpoint Protection Manager, you must have a valid Web Security Service subscription license. Contact your account representative for a Web Security Service license.

- How WSS Traffic Redirection works
- Configuring WSS Traffic Redirection

How WSS Traffic Redirection works

Symantec Endpoint Protection updates the proxy configuration browser settings using WSS Traffic Redirection feature. Every time a user accesses a website using a web browser, the browser sends all web browser traffic through the nearest cloud-hosted Web Security Service as defined by a Proxy Auto Configuration (PAC) file. Based on the predefined configuration, the Symantec WSS proxy can redirect, allow, or block the traffic.

As of 14.2, you can allow enhanced client authentication with WSS and a more granular control of web traffic, based on the user who sends it.

Browsers that support WSS Traffic Redirection are:

- Microsoft Internet Explorer 9 - 11
- Mozilla Firefox
- Google Chrome
- Microsoft Edge

Note: Macs support Apple Safari, Google Chrome, and Mozilla Firefox.

Configuring WSS Traffic Redirection

1. In Symantec Endpoint Protection Manager, click **Policies > Integrations**, and then open an **Integrations** policy.
2. Click **WSS Traffic Redirection** > **Enable WSS Traffic Redirection**.
3. Under **Proxy auto-configuration (PAC) file URL**, enter a valid PAC file URL.

   You get this URL from the administrator in your network that manages Symantec Web Security Service. You can configure or edit this URL in Symantec Endpoint Protection Manager only.

4 You can add a WSS integration token to gather granular information to create per-user rules.

You can define the traffic interception port if the default of 2968 does not work in your environment.

5 (Optional): Click **Install the Symantec Web Security Service root certificate on clients to facilitate the protection of encrypted traffic** to install the appropriate root certificate on Symantec Endpoint Protection clients to protect encrypted traffic.

6 Click **OK**.

After you assign the policy to client groups, Firefox users must restart the browser for WSS Traffic Redirection settings to apply.

Note: If you click **Mixed control** under **Client User Interface Control Settings** and then click **Customize**, no option exists in the client user interface settings to configure WSS Traffic Redirection.

Chapter 25

Testing security policies

This chapter includes the following topics:

Testing Symantec Endpoint Protection Manager policies

You may need to evaluate Symantec Endpoint Protection or you may need to test the policies before you download them to the client computers. You can test the following functionality using the Symantec Endpoint Protection Manager policies to make sure the product works correctly on the client computers.

Table 25-1 Features that you can test

Feature	See this topic
Virus and Spyware Protection	To test a default Virus and Spyware Protection policy, download the EICAR test virus from: http://www.eicar.org/86-0-Intended-use.html See "Testing a Virus and Spyware Protection policy" on page 568.
SONAR	Download the Socar.exe test file to verify that SONAR works correctly
Insight	How to test connectivity with Insight and Symantec Licensing servers
Intrusion Prevention	Testing a default IPS policy
Application Control	See "Blocking a process from starting on client computers" on page 569. See "Preventing users from writing to the registry on client computers" on page 569. See "Preventing users from writing to a particular file" on page 571. See "Adding and testing a rule that blocks a DLL " on page 572. See "Adding and testing a rule that terminates a process" on page 573.

Testing a Virus and Spyware Protection policy

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

To test a Virus and Spyware Protection policy

1. On the client computer, download the antivirus test file from the EICAR website at the following location:

   http://2016.eicar.org/86-0-Intended-use.html

2. Run the EICAR test file.

   A notification appears that tells you that a risk is found.

3. In Symantec Endpoint Protection Manager, on the **Monitors** page, click **Logs**.
4. On the **Logs** tab, in the **Log type** drop-down list, click **Risk**, and then click **View Log**.
5. On the **Risk Logs** page, the **Virus found event** appears.

Blocking a process from starting on client computers

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

To add a rule that blocks a process from starting on the client computer

1. Open an Application Control policy, and on the **Application Control** pane, click **Add**.
2. In the **Application Control Rule Set** dialog box, in the **Rules** list, select a rule, and on the **Properties** tab, in the **Rule name** text box, type **ftp_ blocked_from_cmd**.
3. To the right of **Apply this rule to the following processes**, click **Add**.
4. In the **Add Process Definition** dialog box, under **Processes name to match**, type **cmd.exe**, and then click **OK**.
5. In the **Application Control Rule Set** dialog box, under the **Rules** list, click **Add Condition > Launch Process Attempts**.
6. On the **Properties** tab, in the **Description** text box, type **no ftp from cmd**.
7. To the right of **Apply this rule to the following processes**, click **Add**.
8. In the **Add Process Definition** dialog box, under **Processes name to match**, type **ftp.exe**, and then click **OK**.
9. In the **Application Control Rule Set** dialog box, on the **Actions** tab, click **Block access**, **Enable logging**, and **Notify user**.
10. Under **Notify user**, type **ftp is blocked if launched from the cmd**.
11. Click **OK** twice, and assign the policy to a group.

    Test the rule.

To test a rule that blocks a process from starting on the client computer

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

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

Preventing users from writing to the registry on client computers

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

To test the functionality:

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

To add a test registry key

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

To prevent users from writing to the registry on client computers

1. Open an Application Control policy, and on the **Application Control** pane, click **Add**.
2. In the **Application Control Rule Set**, under the **Rules** list, click **Add > Add Rule**.
3. On the **Properties** tab, in the **Rule name** text box, type **HKLM_write_not_allowed_from_regedit**.
4. To the right of **Apply this rule to the following processes**, click **Add**.
5. In the **Add Process Definition** dialog box, under **Process name to match**, type **regedit.exe**, and then click **OK**.
6. In the **Application Control Rule Set** dialog box, under the **Rules** list, click **Add > Add Condition > Registry Access Attempts**.
7. On the **Properties** tab, in the **Description** text box, type **registry access**.
8. To the right of **Apply this rule to the following processes**, click **Add**.
9. In the **Add Registry Key Definition** dialog box, in the **Registry key** text box, type **HKEY_LOCAL_MACHINE\software\test**, and then click **OK**.
10. In the **Application Control Rule Set** dialog box, on the **Actions** tab, in the **Read Attempt** group box, click **Allow access**, **Enable logging**, and **Notify user**.
11. Under **Notify user**, type **reading is allowed**.
12. In the **Create, Delete, or Write Attempt** group box, click **Block access**, **Enable logging**, and **Notify user**.
13. Under **Notify user**, type **writing is blocked**.
14. Click **OK** twice, and assign the policy to a group.

    Test the rule.

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

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

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

Preventing users from writing to a particular file

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

You can create an Application and Device Control 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.

To add a rule that prevents users from writing to a particular file

1. Open an Application Control policy, and on the **Application Control** pane, click **Add**.
2. In the **Application Control Rule Set** dialog box, under the **Rules** list, click **Add > Add Rule**.
3. On the **Properties** tab, in the **Rule name** text box, type **1.txt in c read allowed write terminate**.
4. To the right of **Apply this rule to the following processes**, click **Add**.
5. In the **Add Process Definition** dialog box, under **Processes name to match**, type **notepad.exe**, and then click **OK**.
6. In the **Application Control Rule Set** dialog box, under the **Rules** list, click **Add > Add Condition > File and Folder Access Attempts**.
7. On the **Properties** tab, in the **Description** text box, type **file access launched**.
8. To the right of **Apply this rule to the following processes**, click **Add**.
9. In the **Add File or Folder Definition** dialog box, in the text box in the **File or Folder Name To Match** group box, type **c:\1.txt**, and then click **OK**.
10. In the **Application Control Rule Set** dialog box, on the **Actions** tab, in the **Read Attempt** group box, select **Allow access**, and then check **Enable logging** and **Notify user**.
11. Under **Notify user**, type **reading is allowed**.
12. In the **Create, Delete, or Write Attempt** group box, click **Block access**, **Enable logging**, and **Notify user**.

13 Under **Notify user**, type **writing to block Notepad**.

14 Click **OK** twice and assign the policy to the client computer group.

Test the rule.

To test a rule that prevents users from writing to a particular file

1 On the client computer, open File Explorer, locate the c:\ drive, and then click **File > New > Text Document**.

If you create the file by using Notepad, the file is a read-only file.

2 Rename the file as 1.txt.

Make sure that the file is saved to the c:\ folder.

3 In Notepad, open the c:\1.txt file.

You can open the file but you cannot edit it.

Adding and testing a rule that blocks a DLL

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

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

---

Note: Some applications that are written to be "security conscious" may interpret the DLL injection as a malicious act. Take counter measures to block the injection or remove the DLL.

To add a rule that blocks a DLL

1 Open an Application Control policy, and on the **Application Control** pane, click **Add**.

2 In the **Application Control Rule Set** dialog box, under the **Rules** list, click **Add > Add Rule**.

3 On the **Properties** tab, in the **Rule name** text box, type **Block user from opening Microsoft WordPad**.

4 To the right of **Apply this rule to the following processes**, click **Add**.

5 In the **Add Process Definition** dialog box, under **Processes name to match**, type **C:\Program Files\Windows NT\Accessories\wordpad.exe**, and then click **OK**.

6 In the **Application Control Rule Set** dialog box, under the **Rules** list, click **Add > Add Condition > Load DLL Attempts**.

7 On the **Properties** tab, in the **Description** text box, type **dll blocked**.

8 To the right of **Apply to the following DLLs**, click **Add**.

9 In the **Add DLL Definition** dialog box, in the text box in the **DLL name to match** group box, type **MSVCRT.dll**, and then click **OK**.

10 In the **Application Control Rule Set** dialog box, on the **Actions** tab, click **Block access**, **Enable logging**, and **Notify user**.

11 Under **Notify user**, type **Should not be able to load WordPad**.

12 Click **OK** twice and assign the policy to the client computer group.

Test the rule.

To test a rule that blocks a DLL

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

Adding and testing a rule that terminates a process

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

To add a rule that terminates a process

1 Open an Application Control policy, and on the **Application Control** pane, click **Add**.

2 In the **Application Control Rule Set** dialog box, under the **Rules** list, click **Add > Add Rule**.

3 On the **Properties** tab, in the **Rule name** text box, type **Terminates Process Explorer if Process Explorer tries to terminate calc.exe**.

4 To the right of **Apply this rule to the following processes**, click **Add**.

5 In the **Add Process Definition** dialog box, under **Processes name to match**, type **procexp.exe**, and then click **OK**.

6 In the **Application Control Rule Set** dialog box, under the **Rules** list, click **Add > Add Condition > Terminate Process Attempts**.

7 On the **Properties** tab, in the **Description** text box, type **dll stopped**.

8 To the right of **Apply this rule to the following processes**, click **Add**.

9 In the **Add Process Definition** dialog box, in the text box in the **Process name to match** group box, type **calc.exe**, and then click **OK**.

10 In the **Application Control Rule Set** dialog box, on the **Actions** tab, click **Terminate process**, **Enable logging**, and **Notify user**.

11 Under **Notify user**, type **If you try to terminate the calc from procexp, procexp terminates**.

12 Click **OK** twice, and assign the policy to a group.

Test the rule.

To test a rule that terminates a process

1 On the client computer, download and run a free version of the Process Explorer from the following URL:

http://technet.microsoft.com/en-us/sysinternals/bb896653.aspx

2 In Windows, open the Calculator.

3 Open the Process Explorer.

4 In the **Process Explorer** window, right-click the `calc.exe` process, and then click **Kill Process**.

The Process Explorer is terminated.

Testing a default IPS policy

To test the default IPS policy, you must first trigger an event on the client computer.

To test a default IPS policy

1 Rename an executable file (.exe) to a jpeg (.jpg).

2 Upload the .jpg file to a web server\site.

3 On the client computer, use a web browser to open the renamed executable file.

Note: To open the renamed executable file, you must access the web server\site using the IP address. For example, you would type: **http://*web server IP address*/*renamed executable*.jpg**

---

4 On the client, if the IPS policy works correctly, the following events occur:

- You should not be able to open the .jpg file.
- A message in the notification area icon states that the client blocked the .jpg file.

- You can open the Security log and look for a log entry that states that the client blocked the .jpg file.

Section 5

Managing clients from the Symantec Endpoint Protection cloud portal

Chapter 26

Using the Symantec Endpoint Protection cloud portal

This chapter includes the following topics:

Introduction to the Symantec Endpoint Protection 14.2 cloud console

https://embed.ustudio.com/embed/DXPQbyHsEtqf/Uh8109teSTtB

The cloud console introduces advanced visibility and controls to detect and remediate emerging threats in your environment.

The cloud console also leverages Symantec Endpoint Protection's advanced machine learning capabilities to provide visibility into suspicious files and intensive policy-based control of antimalware. Advanced machine learning does not require signatures to make sure that threats are stopped in your environment.

The following is a high-level summary of the features you get when you enroll a Symantec Endpoint Protection Manager domain:

- Discover and block suspicious detections with the Intensive Protection policy
- Product configuration to optimize for low-bandwidth environments
- Integrated false management with central blacklist and whitelist
- Modern cloud console for managing advanced features

See "Enrolling a 14.1/14.2 domain in the cloud console from the Symantec Endpoint Protection Manager console" on page 578.

Enrolling a 14.1/14.2 domain in the cloud console from the Symantec Endpoint Protection Manager console

To use the cloud console, you must first enroll your domain from the Symantec Endpoint Protection Manager console **Home** page.

Note: You can enroll a maximum of 10 domains.

---

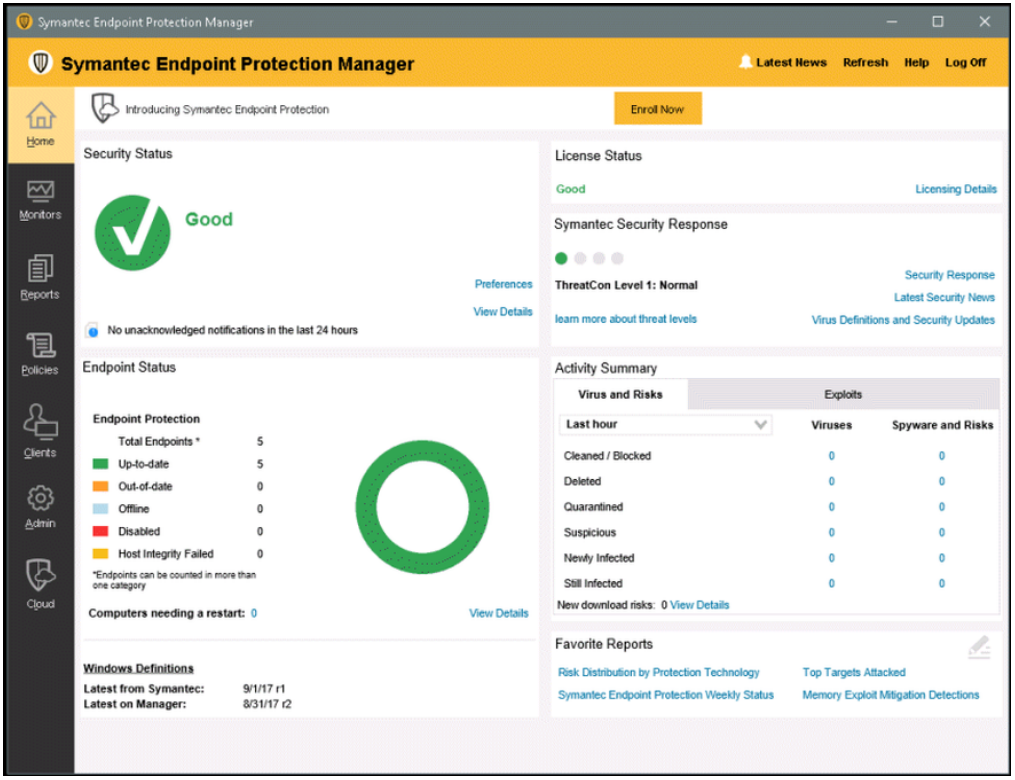
https://embed.ustudio.com/embed/DXPQbyHsEtqf/USbzokAGGD77

Note: **Enrollment with the cloud console installs the Symantec Endpoint Protection Manager Bridge using an .MSI file. Before you begin enrollment, put Application and Device Control into Test (log only) mode and System Lockdown into log-only mode. This situation applies only if such policies apply to the server on which Symantec Endpoint Protection Manager runs, and the policies block .MSI installation.

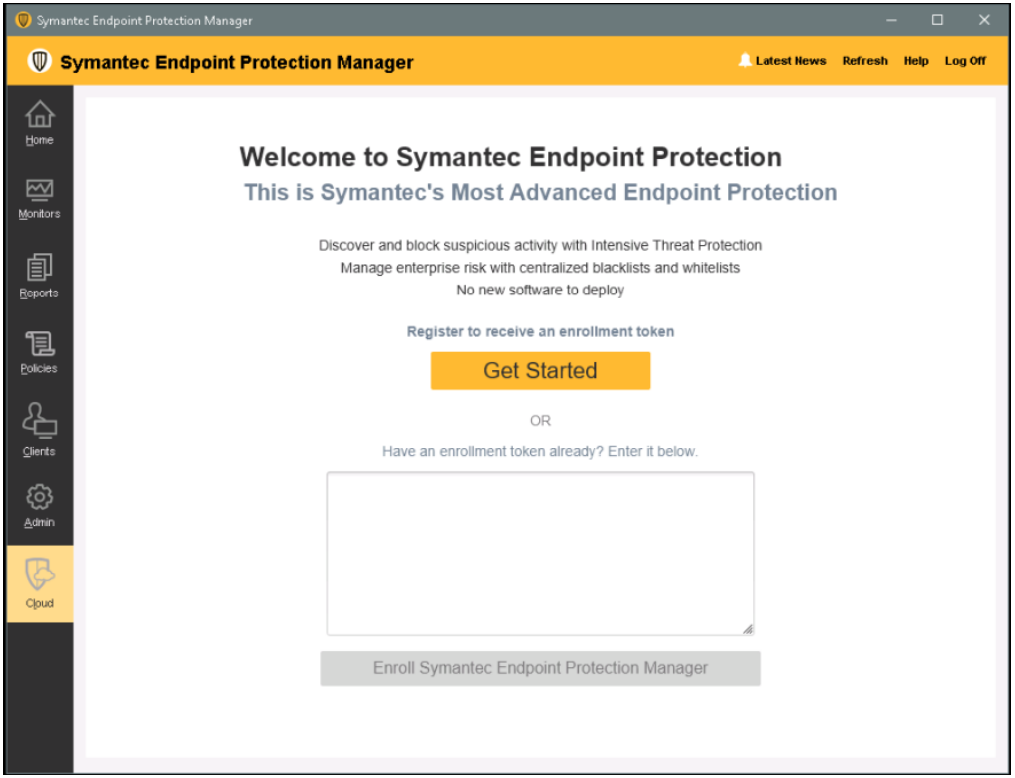
See Enabling and testing default application rules and Setting up and testing the system lockdown configuration before you enable system lockdown.

To start the enrollment

- In the Symantec Endpoint Protection Manager console, press **Enroll Now**.



The enrollment page appears.


Symantec Endpoint Protection Manager
Symantec Endpoint Protection Manager
Latest News
Refresh
Help
Log Off
Home
Monitors
Reports
Policies
Clients
Admin
Cloud
Welcome to Symantec Endpoint Protection
This is Symantec's Most Advanced Endpoint Protection
Discover and block suspicious activity with Intensive Threat Protection
Manage enterprise risk with centralized blacklists and whitelists
No new software to deploy
Register to receive an enrollment token
Get Started
OR
Have an enrollment token already? Enter it below.
Enroll Symantec Endpoint Protection Manager

To get an enrollment code

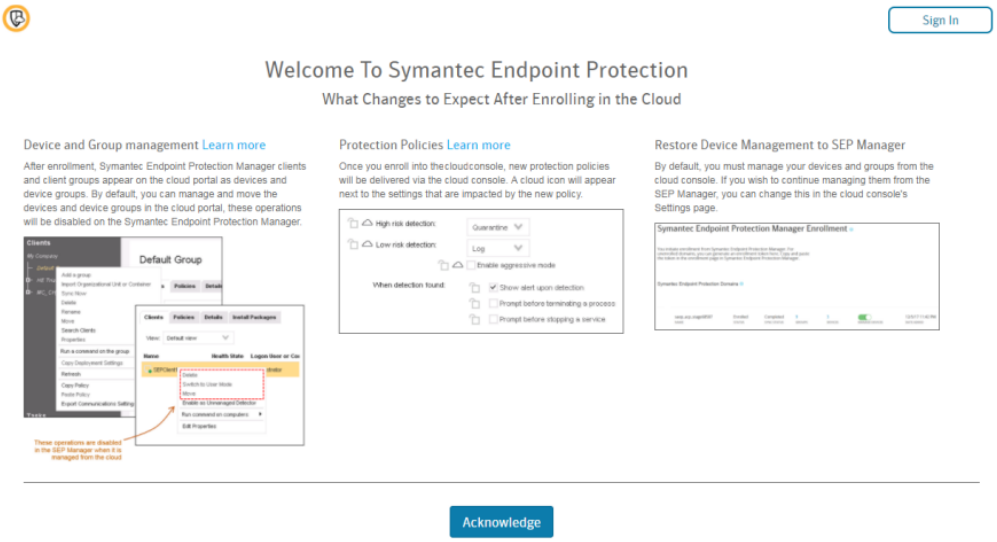
1 On the **Cloud** page in the Symantec Endpoint Protection Manager, press **Get Started**.

Note: If you get a privacy error, you might need to install a certificate. See the following article:

Certificate error when using a web browser to view the management console

---

The acknowledgement page appears.



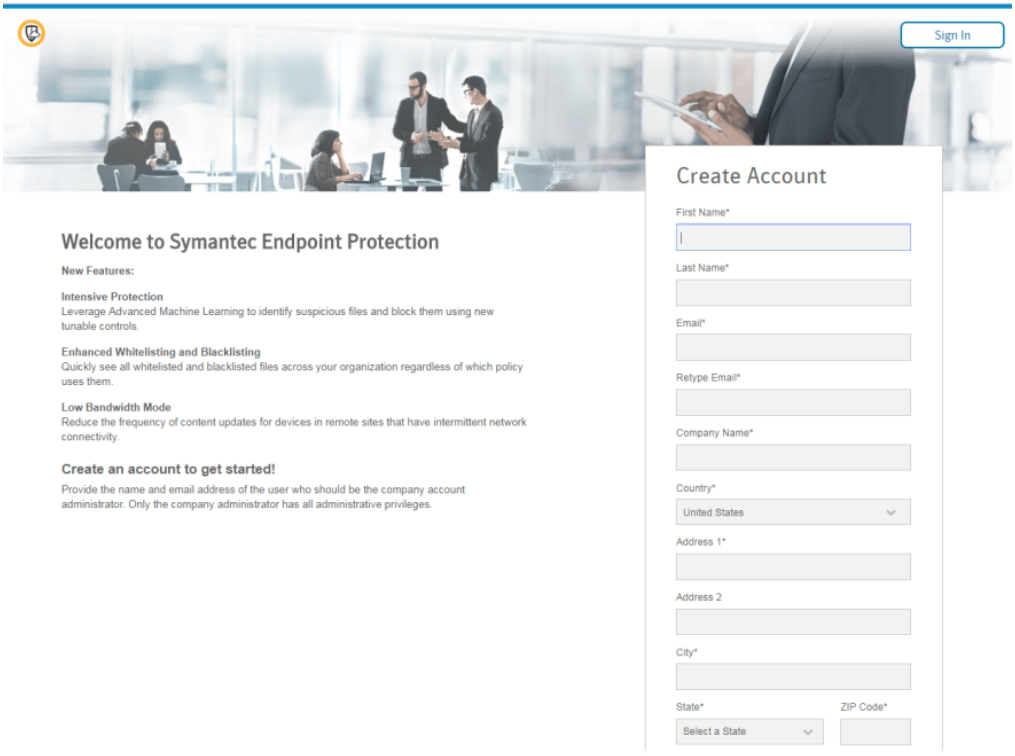
2 Press **Acknowledge**.

Note: Make sure that you read through the page to understand the changes that will happen to device (client) and group management after you enroll the Symantec Endpoint Protection Manager domain.

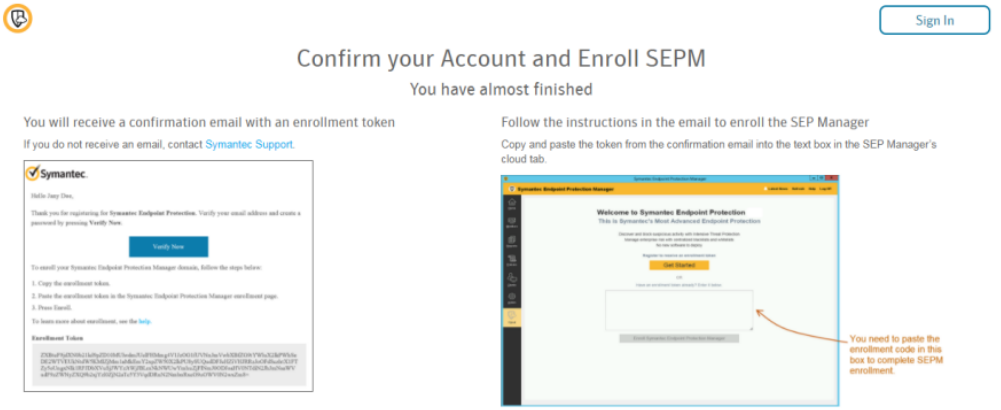
---

3 Create an account, or sign in with existing credentials if you have them.

4 To create an account, enter your information in the form and select **Create Account**. The email address you provide is used to send you verification and domain enrollment information.



A confirmation page appears.



5 When you receive a verification email, select **Verify** in the email to verify your account.

To complete the enrollment

1 Copy the enrollment code from the email and paste the code into the Symantec Endpoint Protection Manager enrollment page.

2 After enrollment, all of your devices appear in the cloud console. Devices include your clients and client groups. By default, the Symantec Endpoint Protection Manager manages the topology. If you want to manage groups and devices from the cloud console, turn off the **Manage Devices** option only for the logged-in domain later in the cloud console in **Settings > Symantec Endpoint Protection Manager Enrollment**.

You should keep this option disabled if you use Active Directory or third-party APIs to manage your devices.

Warning: Whenever you make a change to the device group structure, there is a 10-minute delay before the change appears in Symantec Endpoint Protection Manager. The reverse is also true. The behavior is similar to how Symantec Endpoint Protection Manager replication functions. During the delay, you should not try to make additional topology changes. The changes might not take effect.

Note: When the domain is enrolled, the cloud console always manages cloud-supported policies, regardless of the **Manage Devices** setting.

3 Select **Enroll**.

You get a confirmation message.

4 Now you can use the **Launch** button in the Symantec Endpoint Protection Manager **Home** page banner to log on to the cloud console.

How enrolled-domain cloud console features compare to on-premises Symantec Endpoint Protection Manager

You manage policies in both the cloud console and Symantec Endpoint Protection Manager when your Symantec Endpoint Protection Manager domain is enrolled.

Table 26-1 Feature reference

Symantec Endpoint Protection cloud console	Symantec Endpoint Protection Manager
Devices, device groups Managed by the Symantec Endpoint Protection Manager by default The **Manage Devices** option in enrollment settings controls whether or not the cloud console organizes devices and device groups. **Note:** Whenever you make a change to the device group structure, there is a 10-minute delay before the change appears in Symantec Endpoint Protection Manager. The reverse is also true. The behavior is similar to how Symantec Endpoint Protection Manager replication functions. During the delay, you should not try to make additional topology changes. The changes might not take effect.	**Clients, client groups** When the device master option (**Manage Devices**) for the domain is enabled, you must use the cloud console to organize clients and client groups. If you use the Symantec Endpoint Protection Manager, Active Directory, or you use third-party APIs to manage your devices, you should disable this option. **Note:** The cloud console always manages the policies that it supports, regardless of the **Manage Devices** setting. Symantec Endpoint Protection Manager continues to manage any policies that are not available in the cloud console.
Policy group	No corresponding configuration.

Table 26-1 Feature reference *(continued)*

Symantec Endpoint Protection cloud console	Symantec Endpoint Protection Manager
Policy inheritance In the cloud console, policy inheritance is always enabled. However, you can always directly apply policies to child groups to override the parent policy.	**Policy inheritance** In Symantec Endpoint Protection Manager, you must disable policy inheritance if you want to directly apply a policy to a child group. **Note:** If you unenroll the domain, any MEM policies that you directly applied to child groups from the cloud console are applied to the child groups and their locations regardless of Symantec Endpoint Protection Manager inheritance settings.
Available policies in the cloud console: ■ Intensive Protection policy ■ System policy (low-bandwidth option only) ■ Whitelist policy ■ Blacklist policy ■ MEM policy	**Other policies continue to be managed in Symantec Endpoint Protection Manager:** ■ Firewall policy ■ Intrusion Prevention policy ■ Application and Device Control policy ■ LiveUpdate policy ■ Host Integrity policy ■ Virus and Spyware Protection policy options other than Bloodhound, SONAR heuristics, Download Insight, and scan actions **Note:** Symantec Endpoint Protection 15 provides a fully cloud-managed console.
Intensive Protection policy Automatically applied to Windows clients after domain enrollment (as of 14.0.1) Replaces some settings in Virus and Spyware Protection policies for Windows clients	**Download Insight, Bloodhound and SONAR settings in Virus and Spyware Protection policy** The following settings are not applicable to Symantec Endpoint Protection 14.0.1 clients when the domain is enrolled in the cloud console: ■ Virus and Spyware Protection policy detection actions ■ Bloodhound settings ■ Download Insight sensitivity slider ■ Download Insight prevalence, first-seen, and intranet options ■ SONAR heuristic detection, SONAR aggressive mode, and SONAR suspicious behavior settings These settings are still used for legacy clients and also for 14.0.1 clients and later if you unenroll the domain. **Note:** The default Intensive Protection blocking level is less aggressive than the most aggressive Bloodhound setting in a Virus and Spyware Protection policy. If your current policies specify Bloodhound at its highest level, you might need to increase the Intensive Protection level.

Table 26-1 Feature reference *(continued)*

Symantec Endpoint Protection cloud console	Symantec Endpoint Protection Manager
Whitelist policy Any Whitelist policy that you create in the cloud appears in Symantec Endpoint Protection Manager even if you unenroll the domain.	**Exceptions policy** Items from the cloud console appear in the **Exceptions** list.
Blacklist policy Any Blacklist policy that you create the cloud appears in Symantec Endpoint Protection Manager even if you unenroll the domain. **Note:** The Blacklist policy is a type of application control that uses the SONAR technology in Symantec Endpoint Protection Manager to enforce its rules. It does not use the application control driver in Symantec Endpoint Protection Manager.	**Exceptions policy** Blacklist policies from the cloud console are not scan exceptions. However, blacklist items from the cloud console appear in the **Exceptions** list.
Cloud console exception types ■ Certificate ■ Filename ■ Domain ■ Hash ■ Path ■ Extension ■ IPS Host	**Symantec Endpoint Protection Manager-only exception types** When the domain is enrolled, you can only create exceptions for the types that are not supported in the cloud console. ■ Known risks ■ Extensions ■ Tamper Protection ■ DNS and Host File Change ■ Application to Monitor ■ Linux exceptions ■ Mac exceptions
System policy; low-bandwidth option Default is off.	No corresponding option. The low-bandwidth option can only be enabled or disabled in the cloud console. Symantec Endpoint Protection Manager shows low-bandwidth status. You can see whether or not the low-bandwidth option is enabled in **External Communications > Cloud Settings**. Symantec Endpoint Protection Manager also manages the LiveUpdate AML content that is required for low bandwidth to work.

Table 26-1 Feature reference *(continued)*

Symantec Endpoint Protection cloud console	Symantec Endpoint Protection Manager
Exploit Mitigation policy The policy options are comparable to the options in Symantec Endpoint Protection Manager.	**Memory Exploit Mitigation policy** The policy settings are not configurable when the domain is enrolled in the cloud.
The Low-Bandwidth policy requires low-bandwidth AML content to be downloaded to clients. Content is not controlled or shown in the cloud console.	**Low-bandwidth AML content**. Content type downloaded to Symantec Endpoint Protection Manager or clients for the low-bandwidth option to function.
Browser Isolation policy **Application Isolation policy** **Platform Security policy** **Trusted Updater policy** These policies require a license for Application Isolation.	Devices only receive Application Isolation policies directly from the cloud console. These policies cannot be configured in Symantec Endpoint Protection Manager. **Note:** If your devices are enrolled through Symantec Endpoint Protection Manager, the isolation policies do not appear in Symantec Endpoint Protection Manager. Symantec Endpoint Protection Manager does not collect any logs that are related to these policies.
Application Control policy Requires a license.	**Application and Device Control policy** **System Lockdown** You can continue to use these Symantec Endpoint Protection Manager policies, but there might be some conflicts with Application Control in the cloud.
Administrator roles ■ Super Administrator ■ Limited Administrator ■ Viewer	**Administrator roles** ■ System administrator ■ Administrator (domain-based) ■ Limited administrator (policy based) Cloud console administrators and Symantec Endpoint Protection Manager administrators are not linked in any way.
console timeout You cannot change the timeout period. The timeout is 30 minutes.	**Console timeout** The default is one hour. You can change the timeout.

Table 26-1 Feature reference *(continued)*

Symantec Endpoint Protection cloud console	Symantec Endpoint Protection Manager
Not available. All policy changes happen in real time.	**Heartbeat** option

How Symantec Endpoint Protection Manager interacts with the cloud console

This section lists some expected behaviors that may occur when you enroll a Symantec Endpoint Protection Manager domain in the cloud console.

- Communication and enrollment between the cloud console and Symantec Endpoint Protection Manager
- Licensing, installation, upgrading, databases
- Domains, sites, replication
- Groups, clients, locations
- Policies and inheritance

Communication and enrollment between the cloud console and Symantec Endpoint Protection Manager

- If the Symantec Endpoint Protection Manager connector cannot obtain the access token to the cloud console, it retries every hour.
- Clients that connect through Symantec Endpoint Protection Manager may not immediately display the correct online status in the cloud console. Allow for 5-10 minutes after the online status changes to see an accurate reflection of the current status.
  Checking whether the client is connected to the management server and is protected
- The system time for the management server and the Amazon Web Services (AWS) server must be within 10 minutes of each other. Otherwise, enrollment fails, and you see the following error message:

  ```
  Enrollment in the cloud console cannot complete because the Symantec Endpoint Protection Manger computer date and time does not match the current date and time. Change the setting in the Control Panel, and then retry the enrollment.
  ```

  To resolve the time mismatch, synchronize the Symantec Endpoint Protection Manager server with Network Time Protocol (NTP). See the following for more information:
  http://www.ntp.org

- You can use the following logs to troubleshoot a failed enrollment: `BRIDGE_INSTALL.log`, `catalinaWs.out`, `Cloud-0.log`, `scm-server-0.log`, and `semapisrv_access_log.date.log`. All of these files are in \tomcat\logs, within the Symantec Endpoint Protection Manager installation folder.

See "Enrolling a 14.1/14.2 domain in the cloud console from the Symantec Endpoint Protection Manager console" on page 578.

See "Configuring a management server list for load balancing" on page 736.

Licensing, installation, upgrading, databases

- You do not need a separate license to use or enroll in the cloud console; the cloud console license is free. You only need a license for Symantec Endpoint Protection.
- You cannot upgrade a management server from the cloud console.
- You cannot back up or restore the embedded database or Symantec Endpoint Protection Manager settings from the cloud. You still back up and restore the database and settings in Symantec Endpoint Protection Manager.
- To free up licenses, the Symantec Endpoint Protection Manager database deletes the clients that have not connected to the domain, based on the number of days that you specify. In the cloud console, these clients are automatically deleted after 30 days, and you cannot configure this interval. The clients are deleted first in the Symantec Endpoint Protection Manager database and then in the cloud console. See "Purging obsolete clients from the database to make more licenses available" on page 102.

Domains, sites, replication

- For each site, you enroll one Symantec Endpoint Protection Manager domain per site in the cloud console. You cannot enroll multiple domains even if the domains are in separate sites. You also cannot enroll separate Symantec Endpoint Protection Manager domains if you use the same cloud console account.
- For sites with two Symantec Endpoint Protection Managers that share a SQL Server database and that are configured for failover, you enroll one domain from one of the management servers. The bridge service that communicates between each management server and the cloud console runs on one management server at a time. The service runs on the management server with the higher server priority first. If the first bridge service goes down, the service to the second management server runs instead. You can only manage one domain at a time from the cloud console. The sync between the cloud console and each management server does occur simultaneously.

Table 26-2 displays which site configurations the cloud console supports when you enroll a Symantec Endpoint Protection Manager domain.

Table 26-2 Site configurations that the cloud console supports

Site configuration	Supported on the cloud console
One site, one Symantec Endpoint Protection Manager on one computer with an embedded database only	Yes
One site, one Symantec Endpoint Protection Manager on one computer with a Microsoft SQL Server database on the second computer	Yes
One site, multiple Symantec Endpoint Protection Managers	Yes
Multiple sites, one Symantec Endpoint Protection Manager on each site, with replication*	Yes (as of 14.2)
Multiple sites, multiple Symantec Endpoint Protection Managers on each site, with replication*	Yes (as of 14.2)

* Only one Symantec Endpoint Protection Manager on one of the sites in a replication partnership is supported to enroll with the cloud.

See "Enrolling sites with replication partners in the cloud console" on page 599.

Groups, clients, locations

- If you rename **My Company** in the cloud console, the group name does not change in Symantec Endpoint Protection Manager.
- Cloud-managed features require a managed client. You cannot manage an unmanaged client or apply a policy that uses cloud features to an unmanaged client. If you apply policies that use cloud features to an unmanaged client, the policy defaults to the equivalent legacy Symantec Endpoint Protection options.
- Version 14, 14 MP1, 14 MP2, and legacy 12.1.x client computers appear in the cloud console, but do not support any of the new cloud-based features.
- If the **Manage Devices** option is on in the cloud console, the cloud console manages the devices. If it is off, then Symantec Endpoint Protection Manager manages the devices.
  If you use Active Directory with Symantec Endpoint Protection Manager to manage groups and clients, then Symantec Endpoint Protection Manager automatically manages devices. In this case, you cannot switch **Manage Devices** to the cloud console. This setting returns control of the device organization only to Symantec Endpoint Protection Manager. It does not affect policy protection on any group. You continue to manage advanced policy features from the cloud console.
- Whenever you make a change to the device group structure, there is a 10-minute delay before the change appears in Symantec Endpoint Protection Manager. The reverse is also

true. The behavior is similar to how Symantec Endpoint Protection Manager replication functions. During the delay, you should not try to make additional topology changes.

- If you add a group or policy in the cloud console that contains any of the following special characters: **/ \ * ? < > | : "** , these characters are converted to a dash in the Symantec Endpoint Protection Manager. For example, if you name a group `Europe***`, on Symantec Endpoint Protection Manager, this group is labeled as `Europe---`.
- The cloud console does not support locations. Therefore, if a Symantec Endpoint Protection Manager group has multiple locations and each location uses a different policy (shared or non-shared), then only the default location's policy gets synched up and applied to the equivalent group on the cloud console. After the cloud console syncs back with Symantec Endpoint Protection Manager, that group's policy in the cloud console is applied as a shared policy to all the locations in the equivalent group on the Symantec Endpoint Protection Manager. This process applies to both the Memory Exploit Mitigation policy and the Exceptions policy in the Symantec Endpoint Protection Manager.
- The cloud console does not support a connection over IPv6. Enrollment of Symantec Endpoint Protection Manager over an IPv6 network results in the following error:

  ```
  An error has occurred requesting the status for this enrollment token.
  Symantec Endpoint Protection Manager cannot connect to the cloud console.
  Check the network connection and try again.
  ```

Policies and inheritance

- You can only manage policy settings for 14.0.1/14.1, 14.0.1 MP1, 14.0.1 MP2, and 14.2 clients from the cloud.

  You must still manage policy settings for clients earlier than 14.0.1 directly from Symantec Endpoint Protection Manager. However, there are exceptions. If you apply an Exceptions policy from the cloud, and the client supports the exception type, then the exception applies to the client regardless of version. Memory Exploit Mitigation policies apply to all version 14 clients and later.
- Policies that come from the cloud do not follow the policy inheritance configuration for Symantec Endpoint Protection Manager. Instead, they follow the inheritance rules that are defined in the cloud.
- In the Virus and Spyware Protection policy, a cloud icon appears next to some options when the domain is enrolled in the cloud console. If an Intensive Protection policy is in effect, the policy overrides these options for 14.0.1/14.1, 14.0.1 MP1, 14.0.1 MP2, and 14.2 clients only.
- The first default cloud policies that you create and assign in the cloud console is appended with a `v` and a number (`#`) in Symantec Endpoint Protection Manager, as follows: `Default MEM Policy v1`. If you then unenroll and then reenroll the Symantec Endpoint Protection Manager domain, an additional `v#` is appended to the policy name. For example, `Default`

`MEM Policy v1` may become `Default MEM Policy v1 v1` or `Default MEM Policy v1 v3`.

- For differences between the Symantec Endpoint Protection Manager Exceptions policy and the cloud console Blacklist and Whitelist policies:
  See "How does the Symantec Endpoint Protection Manager Exceptions policy interact with the cloud console?" on page 595.

See "How enrolled-domain cloud console features compare to on-premises Symantec Endpoint Protection Manager" on page 584.

About cloud-based groups and policies (14.1/14.2)

Cloud-based groups

After you enroll in the cloud console, Symantec Endpoint Protection Manager's groups automatically appear in the cloud console. Client computers appear in the cloud console as devices. The cloud console does not support locations.

Cloud-based policies

When you enroll a Symantec Endpoint Protection Manager domain in the cloud console, you can create policies from the cloud console that apply to Symantec Endpoint Protection Manager client groups. These policies are pushed down to Symantec Endpoint Protection Manager, which distributes them to the clients.

You can create the following policies in the cloud console:

- Intensive Protection policy
- Whitelist policy
- Blacklist policy
- System policy, for the low-bandwidth option
- Memory Exploit Mitigation policy

Policy inheritance for Symantec Endpoint Protection Manager groups does not apply to policies from the cloud. You identify the cloud-based policies in the **Clients > Policies** tab by the cloud icon that appears next to the policy description.

Table 26-3 Cloud icons

Icon	Description
	The group does not inherit the policy from its parent in the cloud console. The policy applies directly to the group.

Table 26-3 Cloud icons *(continued)*

Icon	Description
	The group inherits the policy from its parent in the cloud console.

See "How Symantec Endpoint Protection Manager interacts with the cloud console" on page 588.

Updating clients in low-bandwidth environments

What is low-bandwidth mode?

As of 14.1, low-bandwidth mode is a new option for those environments that meet at least one of the following criteria:

- Require infrequent virus and spyware, SONAR, and IPS content updates
- Have low connectivity to the cloud

Low-bandwidth clients receive updates infrequently. Symantec updates low-bandwidth content once a week. In low-bandwidth mode, you can use the aggressive mode policy to tune the security on your endpoints even more.

See "How does Symantec Endpoint Protection use advanced machine learning?" on page 447.

You must be enrolled in the cloud console to use the Low Bandwidth policy. Low Bandwidth is off by default.

- In the cloud console, enable low-bandwidth mode in the System Policy.
- Make sure that LiveUpdate downloads low-bandwidth content.
  Download low-bandwidth content to Symantec Endpoint Protection Manager
- Create a client group that gets low-bandwidth content.
  Creating a group for low-bandwidth clients

After you enable the low-bandwidth mode, you can see its status in the **Clients** tab in the **Default** view and the **Protection Technology** view. You can also generate reports based on low-bandwidth content distribution.

See the section called "Running reports on the clients that run in low-bandwidth mode" on page 595.

Enable low-bandwidth mode

You enable or disable low-bandwidth mode in the cloud console's System Policy.

To enable Low Bandwidth

1. In the cloud console, go to **Policies**.
2. Click the **Show Filters** drop-down and select **Policy Type** to sort by policy type.
3. Select the **Name** of the low-bandwidth policy you want to edit.

Note: When you create a policy, you see the policy page at the completion of the policy creation process.

---

4. Use the slider next to the **Run in low Bandwidth Mode** option to enable or disable **Run in low Bandwidth mode**.
5. Click **Save Policy**.

Download low-bandwidth content to Symantec Endpoint Protection Manager

Advanced Machine Learning content is downloaded and enabled by default. You can use the following procedures to verify that they are enabled.

To download low-bandwidth content to Symantec Endpoint Protection Manager

1. In the Symantec Endpoint Protection Manager console, click **Admin > Local Site > Edit Site Properties**.
2. Click to select the **LiveUpdate** tab, then click **Change Selection** next to **Content Types to Download**.
3. Make sure the box next to **Advanced Machine Learning** is checked.
4. Click **OK > OK** to save the changes.

To include low-bandwidth content in LiveUpdate Content Policy

1. In the Symantec Endpoint Protection Manager console, go to **Policies > LiveUpdate**, and then edit the policy that is assigned to the group that contains the low-bandwidth-enabled clients.
2. Click **LiveUpdate Content**, then double-click **LiveUpdate Content Policy**.
3. Under **Windows Settings**, click **Security Definitions**.
4. Ensure that the **Advanced Machine Learning** box is checked.
5. Click **OK** to save the changes.

See "About the types of content that LiveUpdate downloads" on page 191.

Creating a group for low-bandwidth clients

To create a group for low-bandwidth clients

1. In the cloud console, click **Devices**, and then add a child group under **My Company**.

   If you cannot add a child group, enable **Manage Devices** in the cloud console (**Settings > Symantec Endpoint Protection Manager Enrollment**). Otherwise, add the group in Symantec Endpoint Protection Manager. If you use Active Directory synchronization, add the group through Active Directory.

2. Apply the System Policy to this group that you previously configured for Low Bandwidth. On the device group, click **Apply Policy**, add the System Policy, and then click **Submit**.

3. In the Symantec Endpoint Protection Manager console, ensure that the LiveUpdate Content Policy that you previously configured applies to the group you created. Policy inheritance that you enable or disable in Symantec Endpoint Protection Manager applies only to Symantec Endpoint Protection Manager policies, and not to cloud console device policies.

   You may need to allow some time for the group to sync from the cloud console.

Running reports on the clients that run in low-bandwidth mode

You can run a report to list the clients that receive low-bandwidth content.

To run a report on the clients that run in low-bandwidth mode

1. In the Symantec Endpoint Protection Manager console, click **Reports > Quick Reports**, and then make the following selections:

   - Report type: **Computer Status**
   - Select a report: **Low Bandwidth Content Distribution**

2. Select a time range: **Additional Settings for more options**.

3. Click **Create Report**.

How does the Symantec Endpoint Protection Manager Exceptions policy interact with the cloud console?

How do Exceptions policies work on the cloud console?

The cloud console does not support all the exceptions that the Symantec Endpoint Protection Manager supports. After you enroll a Symantec Endpoint Protection Manager domain in the cloud console, the original Symantec Endpoint Protection Manager Exceptions policy divides into two policy types in the cloud console, based on the types of exceptions. These cloud-based policies are called the Blacklist policy and the Whitelist policy. The exceptions that the cloud policies do not support remain in the Symantec Endpoint Protection Manager Exceptions

policy. After the cloud console and Symantec Endpoint Protection Manager synchronize, the cloud-based policies are imported back into Symantec Endpoint Protection Manager.

For example, assume that in Symantec Endpoint Protection Manager you create a policy that is called *SEPM Exceptions Policy*. This policy includes an Application exception, a Trusted Web Domain exception, and an Application to Monitor exception. After you enroll in the cloud console, the cloud-based exceptions in *SEPM Exceptions Policy* are separated into two policies. These policies are called *Imported SEPM Exceptions Policy (BL)* and *Imported SEPM Exceptions Policy (WL)*. The Blacklist policy is created with the Application exception only, and the Whitelist policy is created with the Application exception and the Domain exception. The original Symantec Endpoint Protection Manager *SEPM Exceptions Policy* retains the Application to Monitor exception. After the cloud console synchronizes with Symantec Endpoint Protection Manager, the Symantec Endpoint Protection Manager displays three policies that are assigned to the same group: *SEPM Exceptions Policy*, *Imported SEPM Exceptions Policy (BL) v1*, and *Imported SEPM Exceptions Policy (WL) v1*.

See “Creating exceptions for Virus and Spyware scans” on page 548.

In addition, the cloud console's Whitelist and Blacklist policies do not support all the actions that the Symantec Endpoint Protection Manager Exceptions policy supports. The Application exception in the cloud console's Whitelist policy only supports the **Ignore** action. The Application exception in the cloud console's Blacklist policy only supports the **Quarantine** action. If you add an Application exception in the Symantec Endpoint Protection Manager Exceptions policy and then enroll Symantec Endpoint Protection Manager in the cloud console, the actions automatically change in the cloud console's policies. The **Log only** action is converted to the **Ignore** action for the Whitelist policy. The **Terminate** and **Remove** actions are converted to the **Quarantine** action. After these policies are imported back into Symantec Endpoint Protection Manager, the management server keeps the action from the cloud console policies.

See “Monitoring an application to create an exception for the application on Windows clients” on page 556.

Which exceptions are supported and not supported on the cloud console?

The cloud console supports the following exceptions on Windows clients:

Blacklist policy:

- Hash (SHA-256)

Whitelist policy:

- Certificate
- Filename
- Domain
- Hash

- File path
- Extension
- IPS Host

After you enroll Symantec Endpoint Protection Manager in the cloud console, the Windows exceptions in the Symantec Endpoint Protection Manager Exceptions policy convert to the following policy type and exception type:

Table 26-4 Windows exceptions and how they convert to cloud console exceptions

Symantec Endpoint Protection Manager Exceptions policy	Blacklist policy	Whitelist policy
Application	Hash (SHA-256 only)	Hash (SHA-256 only)
Certificate	N/A	Certificate
File > Security Risk/SONAR	N/A	Filename
Folder > Security Risk/SONAR	N/A	Path
Trusted Web Domain	N/A	Domain

The following Windows exceptions remain in the Symantec Endpoint Protection Manager Exceptions policy and are not supported in the cloud console:

- Application to Monitor
- Extensions
- File - Application Control
- Folder - Application control
- Known Risks
- Tamper Protection Exception
- DNS or Host File Change Exception

The cloud console does not support Linux client exceptions or Mac client exceptions. All Linux exceptions items and Mac exceptions items remain in the Symantec Endpoint Protection Manager Exceptions policy.

Note: You can also add exceptions directly into the cloud console using a .csv file of checksums that you export from Symantec Endpoint Protection Manager. This file fingerprint 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. Creating a file fingerprint list with checksum.exe

---

See "Which Windows exceptions do I use for what type of scan?" on page 546.

Exceptions that users can add on the Windows client

The Symantec Endpoint Protection Manager Exceptions policy allows you to enable users on the Windows clients to add exceptions (called client restrictions).

If Symantec Endpoint Protection Manager is enrolled in the cloud console, Symantec Endpoint Protection Manager does not display the following client restrictions:

- Application Exception
- File Exception
- Folder Exceptions > Security risk Exception/SONAR Exception
- Trusted Web Domain Exception
- Certificate Exception

Note: In addition, on Windows clients that a cloud-based exceptions policy controls, these exceptions do not appear in the client user interface.

Symantec Endpoint Protection Manager does display the following client restrictions, whether or not Symantec Endpoint Protection Manager is enrolled.

- DNS or Host File Change Exception
- Extension Exception
- Known Risks Exception

See "Restricting the types of exceptions that users can configure on client computers" on page 561.

Issues with enrolling and synchronizing Exceptions policies with the cloud console

- A Blacklist policy or Whitelist policy gets automatically created in the cloud console only if the original Symantec Endpoint Protection Manager Exceptions policy includes the exceptions that the Blacklist policy and the Whitelist policy support. Otherwise, the cloud console ignores the Exceptions policy.
- After enrollment, only assigned Symantec Endpoint Protection Manager Exceptions policies synchronize with the cloud console and then get imported back onto Symantec Endpoint Protection Manager. Unassigned polices remain in Symantec Endpoint Protection Manager as non-cloud-based Exceptions policies. Also, if the assigned Symantec Endpoint Protection Manager Exception policy has no Blacklist exceptions or Whitelist exceptions, then a corresponding empty Blacklist policy and/or empty Whitelist policy gets created in the cloud console for that group.

- After enrollment, you can create and assign non-cloud-based Exceptions policies in Symantec Endpoint Protection Manager. However, these policies must include Symantec Endpoint Protection Manager-based exceptions only, and not cloud-based exceptions. If you create and assign a cloud-based Blacklist policy or Whitelist policy, these policies get synchronized and imported into Symantec Endpoint Protection Manager.
- Exceptions policies that you created in the cloud console remain in Symantec Endpoint Protection Manager after you unenroll the domain. But these cloud-based polices get unassigned from a group in Symantec Endpoint Protection Manager. You can merge them, reassign them, or delete them if you no longer need them.
- If you import a Symantec Endpoint Protection Manager Exceptions policy into the cloud console and that policy has application exceptions, the exceptions are lost after import. You must then manually re-add the application exceptions into the cloud console's Blacklist and Whitelist policies. The cloud console maintains the other types of exceptions, such as the certificate exception.

Enrolling sites with replication partners in the cloud console

How do you enroll a site in the cloud console?

As of version 14.2, you set up replication between one site that is enrolled in the cloud console, and additional sites that are not. You enroll one site as the master site. All other sites can replicate directly with the master site, or replicate with each other. For example, if Site A is the master site, you enroll Site A into the cloud console. You configure Site B and Site C to replicate with Site A. Or, you can configure Site B to replicate with Site A, and configure Site C to replicate with Site B.

Table 26-5 Process for enrolling multiple replicated sites

Task	Description
Step 1: Replicate the two sites before you enroll in the cloud console.	Replicate all policies, groups, and log events before you enroll the master site to avoid any database conflicts. You can also add a replication partner after you enroll the master site in the cloud. The master site can have multiple partner sites. See "Replicating data immediately" on page 750. See "What are sites and how does replication work?" on page 741.
Step 2: Enroll the master site.	Choose and enroll one site as the master site to perform the enrollment and any further actions, such as creating policies. For sites with multiple management servers, you only need to enroll one of the management servers. Any additional management servers are enrolled automatically. You do not enroll the second site, or the partner site, in the cloud console. See "Enrolling a 14.1/14.2 domain in the cloud console from the Symantec Endpoint Protection Manager console" on page 578.
Step 3: Wait for synchronization to occur.	After the enrolled master site and the cloud console synchronize, the following events occur on the master site: ■ The bridge service is installed on all management servers automatically. However, the bridge service is only active on the management server that you used to enroll in the cloud console. ■ The master site synchronizes reporting events with the cloud console. ■ The master site uploads the groups, devices, policies, log events, client packages, and definitions for all clients that are not connected to this site. ■ The master site receives the policies, logs, and commands from the cloud console and immediately passes the data to the clients that communicate with this site. What happens after you enroll a Symantec Endpoint Protection Manager domain into the cloud console
Step 4: Replicate the master site and any partner sites.	Schedule the replication so that both sites have the same enrollment data. After the replication occurs, the following events occur on the partner site: ■ The partner site receives the content from the cloud console based on the replication schedule with the master site. The clients that are connected to the partner site then receive this data. ■ The partner site gets the enrollment details from the master site. These details appear on the **Cloud** page > **Troubleshooting** page. ■ The partner site's management servers do not install the bridge service. Therefore, the partner site does not synchronize directly with the cloud console. See "How to install a second site for replication" on page 748.

Table 26-5 Process for enrolling multiple replicated sites *(continued)*

Task	Description
Step 5: (Optional) Switch control of groups and devices to the cloud console.	By default, when you enroll an unreplicated Symantec Endpoint Protection Manager domain, the cloud console manages the client group structure. By default, when you enroll a replicated site, Symantec Endpoint Protection Manager manages the group structure. ■ If Symantec Endpoint Protection Manager is the master, you can add groups and policies on the master site, which then gets replicated on the partner site. ■ If you make the cloud console the master, first run replication with the partner site. This replication ensures that groups and policies you added on the partner site sync to the cloud console. To switch control to the cloud console, enable the **Manage Devices** option after enrollment in **Settings > Symantec Endpoint Protection Manager Enrollment** in the cloud console.

You cannot perform failover or load balancing for the replicated partner.

See "Setting up failover and load balancing" on page 732.

Note: If you configure Content Analysis System settings, configure them on the master site so that the functionality is available on the cloud console. If you configure CAS on the partner site, the CAS settings do not synchronize with the cloud console.

Configuring Symantec Endpoint Protection to use the Content Analysis System

Removing and restoring replication between the sites that are enrolled in the cloud console

If you remove the partnership between the master site and a partner site, you also remove the relationship with the cloud console.

To restore the partnership with the master site, use the **Add Existing Replication Partner** wizard.

You can also enroll the partner site in the cloud console directly as an individual site. In this case, you must create a different Symantec Cyber Defense Manager account. To restore the partnership with the master site, you must unenroll the partner site. Then, on the master site, reconfigure the partnership with the **Management Server Configuration Wizard**.

Note: As a best practice, keep the partner site as an individual site and do not try to restore the replication with the master site.

See "Disabling replication and restoring replication before and after an upgrade" on page 153.

See “Reinstalling or reconfiguring Symantec Endpoint Protection Manager” on page 756.

Troubleshooting replication for a site in the cloud console

To get information about master site enrollment and replication:

- Look for replication events.
  On the master site, open the **System log** > **Administrative** log type, and look for the **Replication events** event type.
  See “Viewing logs” on page 655.
- Look at the partner site's enrollment status.
  On the partner site, the **Enrollment Status** displays **Enrolled**.
  Other fields such as **Connection Status** display **None**.
  To display the enrollment information, click the **Cloud** page > **Troubleshooting**.

Section 6

Monitoring, reporting, and enforcing compliance

Chapter 27

Managing Host Integrity to enforce security policies

This chapter includes the following topics:

How Host Integrity works

Host Integrity ensures that client computers are protected and compliant with your company's security policies. You use Host Integrity policies to define, enforce, and restore the security of clients to secure enterprise networks and data.

Table 27-1 Process for enforcing security compliance on the client computer

Step	Description
Step 1: The client computer runs a Host Integrity check on the client computer.	The management server downloads the Host Integrity policy to the client computers in the assigned group. The client computers run the Host Integrity check, which compares each computer's configuration with the requirements that you add to the Host Integrity policy. The Host Integrity policy checks for the existence for antivirus software, patches, hot fixes, and other security requirements. For example, the policy may check whether the latest patches have been applied to the operating system. See "Setting up Host Integrity" on page 606.
Step 2: The Host Integrity check passes or fails	■ If the computer meets all of the policy's requirements, the Host Integrity check passes. ■ If the computer does not meet all of the policy's requirements, the Host Integrity check fails. You can also set up the policy to ignore a failed requirement so that the check passes. See "Allowing the Host Integrity check to pass if a requirement fails" on page 613. You can also set up peer-to-peer authentication in the Firewall policy, which can grant or block inbound access to the remote computers that have the client installed. See "Blocking a remote computer by configuring peer-to-peer authentication" on page 615.

Table 27-1 Process for enforcing security compliance on the client computer *(continued)*

Step	Description
Step 3: Non-compliant computers remediate a failed Host Integrity check (optional)	■ If the Host Integrity check fails, you can configure the client to remediate. To remediate, the client downloads and installs the missing software. You can configure either the client to remediate or the end user to remediate in a predefined requirement or a custom requirement. Host Integrity then rechecks that the client computer installed the software. See "Setting up remediation for a predefined Host Integrity requirement" on page 610. ■ If the Host Integrity check that verifies remediation still fails, the client applies a Quarantine policy. You can use a Quarantine policy to apply stricter restrictions to the failed computers. See "Creating a Quarantine policy for a failed Host Integrity check" on page 614. ■ While the client is in the Quarantine location, the Host Integrity check continues to run and to try to remediate. The frequency of the check and remediation settings are based on how you configure the Host Integrity policy. Once the client is remediated and passes the Host Integrity check, the client moves out of the Quarantine location automatically. In some cases, you may need to remediate the client computer manually.
Step 4: The client continues to monitor compliance	The Host Integrity check actively monitors each client's compliance status. If at any time the client's compliance status changes, so do the privileges of the computer. ■ 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 client switches to a location with a different Host Integrity policy while a Host Integrity check is in progress, the client stops checking. The stop includes any remediation attempts. The user may see 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. You can view the results of the Host Integrity check in the Compliance log. See "Viewing logs" on page 655.

Setting up Host Integrity

Use Host Integrity policies to make sure that the client computers in your network meet your organization's security policies.

Table 27-2 lists the steps you need to perform to set up security compliance using Host Integrity policies.

Table 27-2 Tasks to set up Host Integrity policies

Step	Description
Step 1: Add a Host Integrity policy that checks for a requirement on the client computer and enforces a remediation action for non-compliant computers	When you add a new policy, perform the following tasks: 1 Choose which types of requirements you want the client computer to check. Create a separate requirement for each type of software (such as applications, files, and patches). See "About Host Integrity requirements" on page 608. See "Adding predefined requirements to a Host Integrity policy" on page 609. 2 Configure the remediation actions for non-compliant client computers. Remediation requires that the client computer installs or requests the client user to install the required software. See "Setting up remediation for a predefined Host Integrity requirement" on page 610. 3 Set the order in which requirements are checked and the remediation is tried. For example, updates should be completed in a specific order so that all updates are applied before the user has to restart the client computer.
Step 2: Set the options for the Host Integrity check and notifications	■ Configure how often the Host Integrity check runs. See "Configuring the frequency of Host Integrity check settings" on page 612. ■ Configure whether or not users can cancel remediation. See "Allowing users to delay or cancel Host Integrity remediation" on page 611. ■ Set up a notification to appear on the client computer when the Host Integrity check either passes or fails. Use the notification to tell the end user what to do next. For example, the end user may need to allow a new patch to download and install on the client computer. See "Configuring notifications for Host Integrity checks" on page 613.
Step 3: Set up peer-to-peer enforcement	If the client computers being tested for Host Integrity compliance are on the same network as already-compliant client computers, you can set up peer-to-peer enforcement. You primarily use peer-to-peer enforcement for file sharing. See "Blocking a remote computer by configuring peer-to-peer authentication" on page 615.

Table 27-2 Tasks to set up Host Integrity policies *(continued)*

Step	Description
Step 4: Set up a Quarantine policy for non-compliant and unremediated computers (optional)	If the client computer fails the Host Integrity check and does not perform remediation, you can quarantine the computer using a Quarantine policy. See "Creating a Quarantine policy for a failed Host Integrity check" on page 614.

About Host Integrity requirements

When you create a new Host Integrity policy, decide which type of requirements to add.

Each requirement specifies the following items:

- What conditions to check
  For example, a requirement would check whether the latest set of virus definitions is installed on the client computer.
- What remediation actions the client takes if the client fails to pass the condition's requirements
  For example, the remediation action can include a URL where the client can download and install the missing virus definitions.

Table 27-3 lists the types of requirements you can use.

Table 27-3 Requirement types for Host Integrity policies

Type	Description
Predefined requirements	Use a predefined requirement to check that a specific application or file is installed and runs on the client. A predefined requirement checks for the status of any of the following types of applications: antivirus software, antispyware software, a firewall, a patch, or a service pack. For example, a patch requirement checks that the client computers run a specific operating system patch. If the predefined requirement does not have enough detail, add a custom requirement and write a script. See "Adding predefined requirements to a Host Integrity policy" on page 609.

Table 27-3 Requirement types for Host Integrity policies *(continued)*

Type	Description
Custom requirements from templates	Templates are predefined custom requirements that Symantec wrote for commonly performed tasks. For example, the client can check that a password has been changed in the last 42 days. You can also use the templates as a basis for writing a custom requirement script. Template requirements are available through the Host Integrity policy LiveUpdate service. You must first set up LiveUpdate to download the Host Integrity templates to the management server. See "Adding a custom requirement from a template" on page 616. See "Downloading content from LiveUpdate to the Symantec Endpoint Protection Manager" on page 186.
Custom requirements	Use a custom requirement if neither a predefined requirement nor the templates provide the kind of check that you need. Custom requirements include the same fields as predefined requirements, but provide more flexibility. For example, you can include an antispyware application that is not included in the predefined list of antispyware applications. 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 Internet Explorer and Mozilla Firefox in one requirement. See "Writing a customized requirement script" on page 617.

See "Setting up Host Integrity" on page 606.

Adding predefined requirements to a Host Integrity policy

A predefined requirement in a Host Integrity policy checks that the client computer runs any of several types of applications such as: antivirus, antispyware, firewall, and so on.

You determine the particular application, such as specific patches for the Windows 7 operating system. You then specify the path where the client computers should get the patch.

To add predefined requirements to a Host Integrity policy

1. In the console, open a Host Integrity policy.
2. On the **Host Integrity policy** page, click **Requirements > Add**.
3. In the **Add Requirement** dialog box, click the **Select requirement** drop-down list, select a predefined requirement, and then click **OK**.

4 Configure the settings and remediation options for the requirement, and then click **OK**.

See "Setting up remediation for a predefined Host Integrity requirement" on page 610.

For more information, click **Help**.

5 Click **OK**.

6 Assign the policy to groups or locations.

7 Click **OK**.

See "Adding a custom requirement from a template" on page 616.

See "Writing a customized requirement script" on page 617.

Enabling and disabling Host Integrity requirements

When you add requirements to a Host Integrity policy, the requirements are enabled by default. You must disable them from being used until they are needed. For example, 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 and click **Requirements**.

2 On the **Requirements** page, 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.

3 Click **OK**.

See "Setting up Host Integrity" on page 606.

Setting up remediation for a predefined Host Integrity requirement

If the Host Integrity check on a client shows that a requirement failed, you can configure the policy to restore the necessary files. The client restores files by downloading, installing, or running the required applications to meet the requirement. The client computer can then pass the Host Integrity check.

You set up remediation in the same dialog box in which you add a predefined requirement. You specify both the path from which the client downloads the remediation files and how the remediation process is implemented.

You can also enable users to have some control over when they remediate their computers. For example, a restart may cause users to lose their work, so users may want to delay remediation until the end of the day.

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`.

To set up remediation for a predefined Host Integrity requirement

1. In the console, open a Host Integrity policy, and add a predefined requirement.

   See "Adding predefined requirements to a Host Integrity policy" on page 609.

2. In the **Add Requirement** dialog box, click **Install the <requirement type> if it has not been installed on the client**.
3. Click **Download the installation package**.
4. In the **Download URL** text box, type the URL from where the installation file gets downloaded to the client computer.
5. In the **Execute the command** text box, do one of the following tasks:
   - If you want the client user to run the installation, leave the text box blank.
   - If you want the installation to run automatically, type **%F%**.
     The **%F%** variable represents the last downloaded file. You can use any command that can be run from **Start** > **Run**. For example, to install a patch for Vista, type the command **%Systemroot%\system32\wusa.exe /quiet /norestart %F%**.
6. Optionally set the options to delay or cancel remediation, and then click **OK**.

   See "Allowing users to delay or cancel Host Integrity remediation" on page 611.

7. Click **OK**.

See "Allowing the Host Integrity check to pass if a requirement fails" on page 613.

Allowing users to delay or cancel Host Integrity remediation

You can allow the user to delay remediation to a more convenient time. If users must restart their computers after they install the software for a requirement, they may want to wait to restart their computers until later.

If the user delays remediation, any of the following events can happen:

- The client logs the event. The Host Integrity status is shown as failed because the requirement is not met. The user can manually run a new Host Integrity check at any time from the client.
- The Host Integrity check remediation message window does not appear again until the client runs another Host Integrity check. If the user has chosen to be reminded in five minutes, but the Host Integrity check runs every 30 minutes, the message window does not appear until 30 minutes. 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 delays the remediation before the next Host Integrity check, the user selection is overridden.
- If the user delays a remediation action and the client receives an updated policy, the amount of time available for remediation is reset to the new maximum.

To allow users to delay or cancel Host Integrity remediation

1. In the console, open a Host Integrity policy and add a requirement.

   See "Adding predefined requirements to a Host Integrity policy" on page 609.

2. In the **Add Requirement** dialog box, set up remediation.

   See "Setting up remediation for a predefined Host Integrity requirement" on page 610.

3. On the dialog box for the requirement, do one of the following tasks, and then click **OK**:
   - To let the client user delay a file from being downloaded, check **Specify wait time before attempting the download again if the download fails**.
   - To let the client user cancel remediation, check **Allow the user to cancel the download for Host Integrity remediation**.
4. Click **OK**.
5. Click **Advanced Settings**.
6. On the **Advanced Settings** page, under **Remediation Dialog Options**, configure the options for canceling the remediation.
7. To add a custom message on the client computer, click **Set Additional Text**.

   The message you type appears on the client remediation window if the user clicks **Details**.
8. Click **OK**.

Configuring the frequency of Host Integrity check settings

You can configure how the Host Integrity check is carried out and how the results are handled.

After you add or update a Host Integrity policy, the policy is downloaded to the client at the next heartbeat. The client then runs the Host Integrity check.

If the user switches to a location with a different 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.

To configure the frequency of Host Integrity check settings

1. In the console, open a Host Integrity policy, and click **Advanced Settings**.
2. On the **Advanced Settings** page, under **Host Integrity Checking Options**, set the Host Integrity check frequency.
3. Click **OK**.

See "Adding predefined requirements to a Host Integrity policy" on page 609.

See "Allowing the Host Integrity check to pass if a requirement fails" on page 613.

Allowing the Host Integrity check to pass if a requirement fails

Users may need to continue working even if their computers fail the Host Integrity check. You can let the Host Integrity check pass even if a specific requirement fails. The client logs the results but ignores the results.

You apply this setting 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.

To allow the Host Integrity check to pass if a requirement fails

1. In the console, open a Host Integrity policy.
2. Add a predefined requirement or a custom requirement, and then click **OK**.

   See "Adding predefined requirements to a Host Integrity policy" on page 609.

   See "Writing a customized requirement script" on page 617.
3. On the dialog box for the requirement, check **Allow the Host Integrity check to pass even if this requirement fails**, and then click **OK**.
4. Click **OK**.

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-hand 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 delay the remediation.

See "Allowing users to delay or cancel Host Integrity remediation" on page 611.

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 failing**.
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**.

Creating a Quarantine policy for a failed Host Integrity check

You use a Quarantine policy for the client computers that fail the Host Integrity check, try to remediate, and then fail remediation again. After the client computer fails remediation, it automatically switches to a Quarantine location, where a Quarantine policy is applied to the computer. You use a Quarantine policy to apply stricter restrictions to the failed computers. You can use any type of protection policy for the Quarantine policy. For example, you can apply a Quarantine Firewall policy that blocks a computer's access to the Internet.

While the client computer is in the Quarantine location, you can configure the Host Integrity check to continue to run and try to remediate the computer. You may also need to remediate the computer manually.

To create a Quarantine policy for a failed Host Integrity check

1. In the console, click **Clients**, and then click the **Policies** tab.
2. On the **Policies** tab, next to **Quarantine Policies when Host Integrity Fails**, click **Add a policy**.
3. In the **Add Quarantine Policy** dialog box, choose a policy type and then click **Next**.
4. Choose whether to use an existing policy, create a new policy, or import a policy file, and then click **Next**.
5. 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 "Setting up remediation for a predefined Host Integrity requirement" on page 610.

See "About Host Integrity requirements" on page 608.

Blocking a remote computer by 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. You can use this enforcement technique when the remote computer is physically remote. The technique leverages advanced capabilities of the Symantec Endpoint Protection firewall to enhance access to shared files.

The Host Integrity check verifies the following characteristics of the remote computer:

- The remote computer has Symantec Endpoint Protection installed.
- The remote computer passed the Host Integrity check.

If the remote computer passes the Host Integrity check, the authenticator allows inbound connections from the remote computer.

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 do 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 Network and Host Exploit Mitigation Traffic log.

Note: Peer-to-peer authentication works in server control and mixed control, but not in client control.

To block a remote computer by configuring peer-to-peer authentication

1. In the console, open a Firewall policy.
2. On the **Firewall policy** page, click **Peer-to-Peer Authentication Settings**.
3. On the **Peer-to-Peer Authentication Settings** page, check **Enable peer-to-peer authentication**.
4. Configure each value 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. Click **OK**.
10. If you are prompted, assign the policy to a group.

See "Creating a firewall policy" on page 340.

See "Setting up Host Integrity" on page 606.

See "Preventing users from disabling protection on client computers" on page 327.

Adding a custom requirement from a template

Instead of writing custom requirements from scratch, you can add common custom requirements that Symantec created. You use LiveUpdate to download Host Integrity content to the management server. The Host Integrity content includes templates. You then add the custom requirements from the templates to the Host Integrity policy.

To get the latest Host Integrity templates, you must configure a LiveUpdate Content policy to download Host Integrity content.

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.

To add a custom requirement from a template

1. In the console, open a Host Integrity policy.
2. On the **Host Integrity policy** page, click **Requirements > Add**.
3. In the **Add Requirement** dialog box, click the **Select requirement** drop-down list, select a predefined requirement, and then click **OK**.
4. In the **Host Integrity Online Updating** dialog box, expand **Templates**, and then select a template category.
5. Next to each template you want to add, click **Add**.
6. Click **Import**.
7. Click **OK**.

See "About Host Integrity requirements" on page 608.

See "Downloading content from LiveUpdate to the Symantec Endpoint Protection Manager" on page 186.

See "Reverting to an older version of the Symantec Endpoint Protection security updates" on page 213.

Writing a customized requirement script

Custom requirements provide more flexibility than a predefined requirement. For example, you can add an application that is not included in the predefined lists of applications.

To build a custom requirement, you add one or more functions or **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.

When you add many different conditions in one script to check for, 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 customized requirement script

1. In the console, open a Host Integrity policy.
2. On the **Host Integrity policy** page, click **Requirements > Add**.

3 In the **Add Requirement** dialog box, click the **Select requirement** drop-down list, select a predefined requirement, and then click **OK**.

4 In the **Custom Requirement** dialog box, type a name for the requirement.

The requirement name appears 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.

5 To add a condition, under **Customized Requirement Script**, click **Add**, and then click **IF..THEN**.

Note: If you first add a function or an **IF..THEN** statement without filling out the fields, an error appears. If you do not want to add the statement, right-click the statement and click **Delete**.

---

6 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.

7 Under the **Select a condition** drop-down list, specify the additional information that is required.

8 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.

9 Click any of the following options:

- **IF..THEN**
  Use a nested **IF..THEN** statement to define conditions to check and actions to take if the condition is evaluated as true.
- **Function**
  Use a function to define a remediation action, such as downloading a file.
- **Return**
  Use a return statement to specify whether the results of the evaluation of the condition pass or fail. Every custom requirement must end with a pass or fail statement.
- **Comment** (optional)
  Use a comment to explain the functionality of the conditions, functions, or statements that you add.

10 In the right-hand pane, define the criteria that you added.

For more information on these options, click **Help**.

11 To add more nested statements, conditions, or functions, under **Customized Requirement Script**, right-click the node, and then click **Add**.

12 Repeat steps 9 to 11 as needed.

13 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**.

14 Click **OK**.

See "Creating a test Host Integrity policy with a custom requirement script" on page 622.

See "Adding predefined requirements to a Host Integrity policy" on page 609.

About registry conditions

You can specify which Windows registry settings to check as part of an **IF..THEN** statement for a customized requirement. 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.

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`

Writing a custom requirement to run a script on the client

In a 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 write a custom requirement to run a script on the client

1. In the console, open a Host Integrity policy.
2. On the **Host Integrity policy** page, click **Requirements > Add**.
3. In the **Add Requirement** dialog box, click the **Select requirement** drop-down list, select a predefined requirement, and then click **OK**.

   See "Writing a customized requirement script" on page 617.
4. In the **Custom Requirement** dialog box, under **Customized Requirement Script**, select the node where you want to add the function.
5. Click **Add**, and then click **Function**.
6. Click **Utility: Run a script**.
7. Enter a file name for the script, such as **myscript.js**.
8. Type the content of the script.
9. In the **Execute the command** text field, type the command to use to execute the script.

   Use **%F** to specify the script file name. The script executes in system context.
10. 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.

11 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.

12 Optionally, uncheck **Show new process window** if you do not want to see a window that shows the requirement running the script.

Writing a custom requirement to set 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. You could set the script to run as follows:

- When the client receives a new profile
- When the user manually runs a Host Integrity check

To write a custom requirement to set the timestamp of a file

1 In the console, open a Host Integrity policy.

2 On the **Host Integrity policy** page, click **Requirements > Add**.

3 In the **Add Requirement** dialog box, click the **Select requirement** drop-down list, select a predefined requirement, and then click **OK**.

See "Writing a customized requirement script" on page 617.

4 In the **Custom Requirement** dialog box, under **Customized Requirement Script**, select the node where you want to add the function.

5 Click **Add**, and then click **Function**.

6 Click **Utility: Set Timestamp**.

7 Type a name up to 255 characters long for the registry setting that stores the date and the time information.

For example, enter **Date and time of last file update:**

To compare the current time to the stored time value

1 Write a custom requirement script.

See "Writing a customized requirement script" on page 617.

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.

Writing a custom requirement to increment 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 write a custom requirement to increment the registry DWORD value

1 In the console, add a Host Integrity policy with a custom requirement script.

See "Writing a customized requirement script" on page 617.

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: Increment registry DWORD value**.

5 Enter the registry key to check in the **Registry key** field.

6 Enter a value name to be checked in the **Value name** field.

7 Click **OK**.

Creating a test Host Integrity policy with a custom requirement script

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.

Complete the following tasks:

- Add a Host Integrity policy with a custom requirement script that checks for the operating system on the client computer.
  See "To create a test Host Integrity policy with a custom requirement script" on page 623.
- Test the Host Integrity policy you have created.
  See "To test the Host Integrity policy on the client computer" on page 623.

To create a test Host Integrity policy with a custom requirement script

1. In the console, open a Host Integrity policy.
2. On the **Host Integrity policy** page, click **Requirements > Add**.
3. In the **Add Requirement** dialog box, click the **Select requirement** drop-down list, select a predefined requirement, and then click **OK**.
4. In the **Name** box, type a name for the custom requirement.
5. In the **Custom Requirement** dialog box, under **Customized Requirement Script**, right-click **Insert statements below**, and then click **Add > IF..THEN**.
6. In the right pane, in the **Select a condition** drop-down list, click **Utility: Operating System is**.
7. Under **Operating system**, check one or more operating systems that your client computers run and that you can test.
8. Under **Customized Requirement Script**, right-click **THEN //Insert statements here**, and then click **Add > Function > Utility: Show message dialog**.
9. In the **Caption of the message box** field, type a name to appear in the message title.
10. In the **Text of the message box** field, type the text that you want the message to display.
11. In the left pane, under **Customized Requirement Script**, click **Pass**.
12. In the right pane, under **As the result of the requirement, return**, check **Fail**, and then click **OK**.
13. Click **OK**.
14. In the **Host Integrity Policies** dialog box, in the left panel, click **Assign the policy**.
15. In the **Assign Host Integrity Policy** dialog box, select the groups to which you want to assign the policy, and click **Assign**.

    In the **Assign Host Integrity Policy** dialog box, click **Yes** to assign the Host Integrity policy changes.

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 the Host Integrity policy on the client computer

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 the computer that runs the client 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 "Writing a customized requirement script" on page 617.

See "Writing a custom requirement to increment a registry DWORD value" on page 622.

See "Writing a custom requirement to run a script on the client" on page 620.

Chapter 28

Monitoring protection with reports and logs

This chapter includes the following topics:

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?

Table 28-1 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. ■ View the number of clients that did not get installed. See "Running a report on the deployment status of clients" on page 631. ■ View the number of computers that are offline. See "Finding offline computers" on page 629. ■ Obtain a count of detected viruses and other security risks and view details for each virus and security risk. See "Viewing risks" on page 631. ■ Obtain a count of unprotected computers in your network and view the details for each computer. See "Viewing system protection" on page 634. ■ View the number of computers with up-to-date virus and spyware definitions. See "Viewing system protection" on page 634. ■ View the real-time operational status of your client computers. See "Viewing the protection status of client computers" on page 247. ■ Review the processes that run in your network. See "Monitoring SONAR detection results to check for false positives" on page 500. ■ 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 in your network" on page 630. ■ 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 the license status in Symantec Endpoint Protection Manager" on page 100. See "Viewing a daily or weekly status report" on page 633.

Table 28-1 Tasks for monitoring endpoint protection *(continued)*

Task	Description
Locate which client computers need 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 634. ■ View the number of computers with out-of-date virus and spyware definitions. See "Viewing system protection" on page 634. ■ Find the computers that have not been scanned recently. See "Finding unscanned computers" on page 629. ■ View attack targets and sources. See "Viewing attack targets and sources" on page 632. ■ View event logs. See "Viewing logs" on page 655.
Protect your client computers	You can run commands from the console to protect the client computers. See "Running commands on client computers from the console" on page 253. For example, you can eliminate security risks on client computers. See "Checking the scan action and rescanning the identified computers" on page 407.
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 671.
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 649. See "How to run scheduled reports" on page 652. See "Saving and deleting custom reports" on page 651. See "Configuring reporting preferences" on page 635.

Table 28-1 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 728. ■ Specify how many log entries the client computer can keep in the database, and how long to keep them. See "Specifying the log size and how long to keep log entries in the database" on page 729. ■ Filter the less important risk events and system events out so that less data is forwarded to the server. See "Modifying log handling and notification settings on Windows computers" on page 478. ■ 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 "Updating policies and content on the client using push mode or pull mode" on page 165. ■ 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 730.
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 727. See "Exporting data to a Syslog server" on page 726. See "Viewing logs from other sites" on page 660.
Troubleshoot issues with reports and logs	You can troubleshoot some issues with reporting. See "Troubleshooting reporting issues" on page 777.

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.

Finding unscanned computers

You can list the computers that need scanning.

See "Monitoring endpoint protection" on page 625.

To find unscanned computers

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

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

3. Click **Create Report**.

Finding offline computers

You can list the computers that are offline.

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 connectivity problems between Symantec Endpoint Protection Manager and the Symantec Endpoint Protection client" on page 765.

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 **Additional 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.

Generating a list of the Symantec Endpoint Protection versions installed 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 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 webpage archive format.

See "Printing and saving a copy of a report" on page 654.

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**.

To generate a detailed list of client computers, including Symantec Endpoint Protection software versions

1 In the console, click **Monitors**, and then click the **Logs** tab.

2 For **Log type**, select **Computer Status**.

3 Adjust the **Time range** if desired, and then click **View log**.

4 Scroll to find the column **Version**. Click on the header to sort by version number.

Click **View Applied Filters** to adjust the log filters. Click **Export** to export the list. Click a client computer and then click **Details** to see its details.

See "Viewing logs" on page 655.

See "Choosing which method to upgrade the client software" on page 154.

See "Upgrade resources for Symantec Endpoint Protection" on page 144.

Running a report on the deployment status of clients

You can run several reports on the deployment status of your clients. For example, you can see how many clients were successfully or unsuccessfully installed. You can also see which clients have which protection technologies installed on them, along with system information about the client computers.

See "Monitoring endpoint protection" on page 625.

To view the status of deployed clients

1. In the console, click **Reports**.
2. On the **Quick Reports** tab, click the **Computer Status** report type, and then click one of the following reports:
   - For the deployment status of the clients, click **Deployment Report**.
   - For the protection status of the clients, click **Client Inventory Details**.
3. Click **Create Report**.

Viewing risks

You can get information about the risks in your network.

See "Monitoring endpoint protection" on page 625.

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 attack targets and sources

You can view attack targets and sources.

See “Monitoring endpoint protection” on page 625.

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 and Host Exploit Mitigation**.
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 and Host Exploit Mitigation**.
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 and Host Exploit Mitigation**.
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**.

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 625.

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 625.

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.

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.

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 standalone web browser

You can access the **Home**, **Monitors**, and **Reports** pages from a standalone web browser that is connected to your management server. However, all of the other console functions are not available when you use a standalone 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.
- Your user name and password for the management server.

Note: Check the system requirements for the minimum browser version that is supported with the Symantec Endpoint Protection version in use. Earlier web browser versions are not supported.

Release notes, new fixes, and system requirements for all versions of Endpoint Protection

---

To log on to reporting from a standalone web browser

1. Open a web browser.
2. Type the default reporting URL into the address text box in the following format:

   https://*SEPMServer*:8445/reporting

   Where *SEPMServer* is the host name or IP address of the management server. For a list of supported web browsers, see Release notes, new fixes, and system requirements for all versions of Endpoint Protection.

   IP address includes IPv4 and IPv6. You must enclose the IPv6 address with square brackets. For example: **https://[*SEPMServer*]:8445**

   Note: When you enter 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.

   If you use 12.1 and migrated from version 11, the Symantec Endpoint Protection version 11 default reporting URL was http://*SEPMServer*:8014/reporting. 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 Symantec Endpoint Protection Manager 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.

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.

Table 28-2 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.
Compliance	Displays the information about how many clients passed or failed the Host Integrity check.
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.
Deception	Displays the information about Deception activity, such as top computers or users that report Deception activity, and top Deceptors triggered.

Table 28-2 Report types available as quick reports and scheduled reports *(continued)*

Report type	Description
Network and Host Exploit Mitigation	Displays the information about intrusion prevention, attacks on the firewall, firewall traffic and packets, and Memory Exploit Mitigation. The Network and Host Exploit Mitigation 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. Memory Exploit Mitigation events list which mitigation techniques terminated an application or blocked an exploit from attacking an application.
Risk	Displays the information about risk events on your management servers and their clients. It includes information about SONAR 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.

See "Running and customizing quick reports" on page 649.

See "How to run scheduled reports" on page 652.

The following section describes the reports by name and their general content. You can configure Basic Settings and Advanced Settings for all reports to refine the data you want to view. You can also save your custom filter with a name to run the same custom report at a later time.

Table 28-3 Audit reports

Report name	Description
Policies Used	This report displays the policies that clients and locations use currently. Information includes the domain name, group name, and the serial number of the policy that is applied to each group.

Table 28-4 Application and Device Control reports

Report name	Description
Top Groups With Most Alerted Application Control Logs	This report consists of a pie chart with the relative bars. It shows the groups with the application control logs that have generated the largest number of security alerts.
Top Targets Blocked	This report consists of a pie chart with the following targets, if applicable: ■ Top Files ■ Top Registry Keys ■ Top Processes ■ Top Modules (dlls)
Top Devices Blocked	This report consists of a pie chart that shows the devices most frequently blocked from access to your network.

Table 28-5 Compliance reports

Report name	Description
Host Integrity Status	This report displays the clients that have passed or failed the Host Integrity check that runs on their computer.
Clients by Compliance Failure Summary	This report consists a bar chart that shows: ■ A count of the unique workstations by the type of control failure event, such as antivirus, firewall, or VPN ■ The total number of clients in the group
Compliance Failure Details	This report consists of a table that displays unique computers by control failure. It shows the criteria and the rule that is involved in each failure, along with the percentage of clients that are deployed and the percentage that failed.
Non-compliant Clients by Location	This report consists of a table that shows the compliance failure events. These events display in groups that are based on their location. Information includes the unique computers that failed, and the percentage of total failures and location failures.

Table 28-6 Computer Status reports

Report name	Description
Virus Definition Distributions	This report displays the unique virus definitions file versions that are used throughout your network and the number of computers and percentage using each version.

Table 28-6 Computer Status reports *(continued)*

Report name	Description
Computers Not Recently Updated	This report displays a list of all the computers that have not been recently updated. It also displays the computer's operating system, IP address, user name, and the last time its status was changed.
Symantec Endpoint Protection Product Versions	This report displays the list of version numbers for all the Symantec Endpoint Protection product versions in your network. It also includes the domain and server for each, as well as the number of computers and percentage of each.
Intrusion Prevention Signature Distribution	This report displays the IPS signature file versions that are used throughout your network. It also includes the domain and server for each, as well as the number of computers and percentage of each.
Download Protection Signature Distribution	This report displays the download protection signature file versions that are used throughout your network. It also includes the domain and server for each, as well as the number of computers and percentage of each.
SONAR Signature Distribution	This report displays the SONAR signature file versions that are used throughout your network. It also includes the domain and server for each, as well as the number of computers and percentage of each.
Client Inventory	This report consists of a bar chart that displays the total number of computers and percentages of: ■ Operating System ■ Total Memory ■ Free Memory ■ Total Disk Space ■ Free Disk Space ■ Processor Type
Compliance Status Distribution	This report consists of a pie chart with relative bars that show compliance passes and failures by group or by subnet. It shows the number of computers and the percentage of computers that are in compliance.

Table 28-6 Computer Status reports *(continued)*

Report name	Description
Client Online Status	This report consists of pie charts with the relative bars per group or per subnet. It displays the percentage of your computers that are online. Online has the following meanings: ■ For the clients that are in push mode, online means that the clients are currently connected to the server ■ For the clients that are in pull mode, online means that the clients have contacted the server within the last two client heartbeats ■ For the clients in remote sites, online means that the clients were online at the time of the last replication
Clients With Latest Policy	This report consists of pie charts per group or subnet. It displays the number of computers and percentage that have the latest policy applied.
Client Count by Group	This report consists of a table that lists host information by group. It displays the number of clients and users. If you use multiple domains, this information appears by domain.
Security Status Summary	This report reflects the general security status of the network, and displays the number and percentage of computers that have the following status: ■ The Antivirus English is off ■ Auto-protect is off ■ Tamper Protection is off ■ Restart is required ■ A Host Integrity check failed ■ Network Threat Protection is off
Protection Content Versions	This report displays all the proactive protection content versions that are used throughout your network. One pie chart is displayed for each of the following types of protection: ■ Decomposer versions ■ Eraser Engine versions ■ SONAR Content versions ■ SONAR Engine versions ■ Commercial Application List versions ■ Content Handler Engine versions ■ Permitted Application List versions ■ The new content types that Symantec Security Response has added
Symantec Endpoint Protection Licensing Status	This report contains days remaining for trial license expiration and instructions to add new licenses.

Table 28-6 Computer Status reports *(continued)*

Report name	Description
Client Inventory Details	This report contains details of client inventory, such as computer specifications and signatures.
Client Software Rollout (Snapshots) Scheduled report only	This report consists of tables that track the progression of client package deployments. The snapshot information lets you see how quickly the rollout progresses, and how many clients are still not fully deployed.
Clients Online/Offline Over Time (Snapshots) Scheduled report only	This report consists of line charts and tables that shows the number of clients online or offline. One chart displays for each of the top targets. The target is either a group or an operating system.
Clients With Latest Policy Over Time (Snapshots) Scheduled report only	This report consists of a line chart that displays the clients that have the latest policy applied. One chart displays for each of the top clients.
Non-Compliant Clients Over Time (Snapshots) Scheduled report only	This report consists of a line chart that shows the percentage of clients that have failed a host integrity check over time. One chart displays for each of the top clients.
Virus Definition Rollout (Snapshots) Scheduled report only	This report lists the virus definitions package versions that have been rolled out to clients. This information is useful for tracking the progress of deploying new virus definitions from the console.
Deployment Report	This report summarizes the state of client installations and deployments.

Table 28-7 Network and Host Exploit Mitigation reports

Report name	Description
Top Targets Attacked	This report consists of a pie chart that includes information such as the number and percentage of attacks, the attack type and severity, and the distribution of attacks. You can view information using groups, subnets, clients, or ports as the target.
Top Sources of Attack	This report consists of a pie chart that shows the top hosts that initiated attacks against your network. It includes information such as the number and percentage of attacks, the attack type and severity, and the distribution of attacks.
Top Types of Attack	This report consists of a pie chart that includes information such as the number and percentage of events, the group and severity, and the event type and number by group.

Table 28-7 Network and Host Exploit Mitigation reports *(continued)*

Report name	Description
Top Blocked Applications	This report consists of a pie chart that shows the top applications that were prevented from accessing your network. It includes information such as the number and percentage of attacks, the group and severity, and the event type and number by group.
Attacks Over Time	This report consists of one or more line charts that display attacks during the selected time period. For example, if the time range is the last month, the report displays the total number of attacks per day for the past month. It includes the number and percentage of attacks. You can view attacks for all computers, or by the top operating systems, users, IP addresses, groups, or attack types.
Security Events by Severity	This report consists of a pie chart that displays the total number and percentage of security events in your network, ranked according to their severity.
Blocked Applications Over Time	This report consists of a line chart and table. It displays the total number of applications that were prevented from accessing your network over a time period that you select. It includes the event time, the number of attacks, and the percentage. You can display the information for all computers, or by group, IP address, operating system, or user.
Traffic Notifications Over Time	This report consists of a line chart that shows the number of notifications that were based on firewall rule violations over time. The rules that are counted are those where you checked the Send Email Alert option in the Logging column of the Firewall Policy Rules list. You can display the information in this report for all computers, or by group, IP address, operating system, or user.
Top Traffic Notifications	This report consists of a pie chart with relative bars that lists the group or subnet, and the number and percentage of notifications. It shows the number of notifications that were based on firewall rule violations that you configured as important to be notified about. The rules that are counted are those where you checked the Send Email Alert option in the Logging column of the Firewall Policy Rules list. You can view information for all, for the Traffic log, or for the Packet log, grouped by top groups or subnets.
Memory Exploit Mitigation Detections	This report displays the number of memory exploit mitigation types that have been blocked or allowed.

Table 28-7 Network and Host Exploit Mitigation reports *(continued)*

Report name	Description
Full Report	This report gives you the following Network Threat Protection information in a single report: ■ Top Types of Attack ■ Top Targets Attacked by Group ■ Top Targets Attacked by Subnet ■ Top Targets by Client ■ Top Sources of Attack ■ Top Traffic Notifications by Group (Traffic) ■ Top Traffic Notifications by Group (Packets) ■ Top Traffic Notifications by Subnet (Traffic) ■ Top Traffic Notifications by Subnet (Packets) ■ This report includes the information for all domains

Table 28-8 Risk reports

Report name	Description
Infected and At Risk Computers	This report consists of two tables. One table lists computers that have a virus infection, and the other table lists the computers that have a security risk that has not yet been remediated.
Action List	This report consists of a table that shows a count of all the possible actions that were taken when risks were detected. The possible actions are Cleaned, Suspicious, Blocked, Quarantined, Deleted, Pending Repair, Logged Commercial or Forced detections, Newly Infected, and Still Infected. This information also appears on the Symantec Endpoint Protection Home page.
Risk Detections Count	This report consists of a pie chart, a risk table, and an associated relative bar. It shows the number of risk detections by domain, server, or computer. If you have legacy Symantec AntiVirus clients, the report uses the server group rather than the domain.

Table 28-8 Risk reports *(continued)*

Report name	Description
New Risks Detected in the Network	This report consists of a table and a distribution pie chart. For each new risk, the table provides the following information: ■ Risk name ■ Risk category or type ■ First discovered data ■ First occurrence in the organization ■ Scan type that first detected it ■ Domain where it was discovered (server group on legacy computers) ■ Server where it was discovered (parent server on legacy computers) ■ Group where it was discovered (parent server on legacy computers) ■ The computer where it was discovered and the name of the user that was logged on at the time The pie chart shows new risk distribution by the target selection type: domain (server group on legacy computers), group, server (parent server on legacy computers), computer, or user name.
Top Risk Detection Correlation	This report consists of a three-dimensional bar graph that correlates virus and security risk detections by using two variables. You can select from computer, user name, domain, group, server, or risk name for the x and y axis variables. This report shows the top five instances for each axis variable. If you selected computer as one of the variables and there are fewer than five infected computers, non-infected computers may appear in the graph. **Note:** For computers running legacy versions of Symantec AntiVirus, the server group and parent server are used instead of domain and server.
Download Risk Distribution	This report displays the number of files detected by Download Insight and groups them by sensitivity level. Detailed reports are given to files that have been found. You can also group files by URL, web domain, application, and user-allowed before running the report.
Risk Distribution Summary	This report consists of a pie chart and an associated bar graph that displays a relative percentage for each unique item from the chosen target type. For example, if the chosen target is risk name, the pie chart displays slices for each unique risk. A bar is shown for each risk name and the details include the number of detections and its percentage of the total detections. Targets include the risk name, domain, group, server, computer, user name, source, risk type, or risk severity. For computers running legacy versions of Symantec AntiVirus, the server group and parent server are used instead of domain and server.

Table 28-8 Risk reports *(continued)*

Report name	Description
Risk Distribution Over Time	This report consists of a table that displays the number of virus and security risk detections per unit of time and a relative bar.
Risk Distribution by Protection Technology	This report displays the number of virus and security risk detections per protection technology.
SONAR Detection Results	This report consists of a pie chart and bar graphs that display the following information: ■ A list of the applications that are labeled as risks that you have added to your exceptions as permitted in your network ■ A list of the applications that have been detected that are confirmed risks ■ A list of the applications that have been detected but whose status as a risk is still unconfirmed For each list, this report displays the company name, the application hash and the version, and the computer involved. For the permitted applications, it also displays the source of the permission.
SONAR Threat Distribution	This report consists of a pie chart that displays the top application names that have been detected with relative bars and a summary table. The detections include applications on the Commercial Applications List and Forced Detections lists. The first summary table contains the application name and the number and percentage of detections. The summary table displays the following, per detection: ■ Application name and hash ■ Application type, either keylogger, Trojan horse, worm, remote control, or commercial keylogger ■ Company name ■ Application version ■ Number of unique computers that have reported the detection ■ Top three path names in the detection ■ Date of last detection
SONAR Threat Detection Over Time	This report consists of a line chart that displays the number of proactive threat detections for the time period selected. It also contains a table with relative bars that lists the total numbers of the threats that were detected over time.

Table 28-8 Risk reports *(continued)*

Report name	Description
Action Summary for Top Risks	This report lists the top risks that have been found in your network. For each, it displays action summary bars that show the percentage of each action that was taken when a risk was detected. Actions include quarantined, cleaned, deleted, and so on. This report also shows the percentage of time that each particular action was the first configured action, the second configured action, neither, or unknown.
Number of Notifications	This report consists of a pie chart with an associated relative bar. The charts show the number of notifications that were triggered by the firewall rule violations that you have configured as important to be notified about. It includes the type of notifications and the number of each.
Number of Notifications Over Time	This report consists of a line chart that displays the number of notifications in the network for the time period selected. It also contains a table that lists the number of notifications and percentage over time. You can filter the data to display by the type of notification, acknowledgment status, creator, and notification name.
Weekly Outbreaks	This report displays the number of virus and security risk detections and a relative bar per week for each for the specified time range. A range of one day displays the past week.
Comprehensive Risk Report	This report, by default, includes all of the distribution reports and the new risks report. However, you can configure it to include only certain reports. This report includes the information for all domains.
Symantec Endpoint Protection Daily Status	This report contains virus detection, intervention and definition status for network events over the previous 24 hours.
Symantec Endpoint Protection Weekly Status	This report contains licensing status and virus detection statistics for endpoint computers over the previous week. Data reflects cumulative values unless otherwise noted.

Table 28-9 Scan reports

Report name	Description
Scan Statistics Histogram	This report consists of a histogram where you can select how you want the following information in the scan to be distributed: ■ By the scan time (in seconds) ■ By the number of risks detected ■ By the number of files with detections ■ By the number of files that are scanned ■ By the number of files that are omitted from scans You can also configure the bin width and how many bins are used in the histogram. The bin width is the data interval that is used for the group by selection. The number of bins specifies how many times the data interval is repeated in the histogram. The information that displays includes the number of entries and the minimum and the maximum values, as well as the average and the standard deviation. You might want to change the report values to maximize the information that is generated in the report's histogram. For example, you might want to consider the size of your network and the amount of information that you view.
Computers by Last Scan Time	This report shows a list of computers in your security network by the last time scanned. It also includes the IP address and the name of the user that was logged in at the time of the scan.
Computers Not Scanned	This report shows a list of computers in your security network that have not been scanned and provides the following formation: ■ The IP address ■ The time of the last scan ■ The name of the current user or the user that was logged on at the time of the last scan

Table 28-10 System reports

Report name	Description
Top Clients that Generate Errors	This report consists of a pie chart for each warning condition and error condition. The charts show the relative error count and relative warning count and percentage, by client.
Top Servers that Generate Errors	This report consists of a pie chart for each warning condition and error condition. The chart shows the relative error count and relative warning count and percentage, by server.

Table 28-10 System reports *(continued)*

Report name	Description
Database Replication Failures Over Time	This report consists of a line chart with an associated table that lists the replication failures for the time range selected.
Site Status Report	This report shows a real-time summary of the health status of all sites and information on all servers on the local site.
WSS Integration Token Usage	This report summarizes the usage of the integration token for client authentication with WSS Traffic Redirection.

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 **Additional 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 651.

See "Printing and saving a copy of a report" on page 654.

See "How to run scheduled reports" on page 652.

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.

See "Editing the filter used for a scheduled report" on page 653.

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)`.

See "About administrator accounts and access rights" on page 281.

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 additional 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**.

How to run 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 728.

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 run scheduled reports

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**.

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 651.

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 “How to run scheduled reports” on page 652.

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.

See "Running and customizing quick reports" on page 649.

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.

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.

See "Changing timeout parameters for reviewing reports and logs" on page 778.

Reports and logs always appear 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 "About the types of Symantec Endpoint Protection Manager logs" on page 656.

See "Saving and deleting custom logs by using filters" on page 659.

To view a log

1 In the console, 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 **Additional Settings** to limit the number of entries you display.

You can also set any other available **Additional 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 Click **View Log**.

You can also click **Save Filter** to save the filter configuration to generate the same log view at a later date.

About the types of Symantec Endpoint Protection Manager 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.

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 on client computers from the console" on page 253.
- Add several kinds of exceptions.
  See "Creating exceptions from log events" on page 561.
- Delete files from the **Quarantine**.
  See "Using the Risk log to delete quarantined files on your client computers" on page 455.

Table 28-11 describes the different types of content that you can view and the actions that you can take from each log.

Table 28-11 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 Windows clients" on page 556.
Compliance	The compliance logs contain information about client Host Integrity. 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.

Table 28-11 Log types *(continued)*

Log type	Contents and actions
Deception	The Deception log contains information about any activity that the clients send back to Symantec Endpoint Protection Manager as the result of deceptor activity. Deception is a set of tools that you use to present to a potential attacker what appears to be desirable data and an attack vector. You use these tools to quickly detect and stop infiltration attempts. The Deception tools and help file are located in the `/Tools/Deception` folder of the installation file.
Network and Host Exploit Mitigation	The Network and Host Exploit Mitigation logs contain information about intrusion prevention, the firewall, and Memory Exploit Mitigation. The 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.
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. See "About SONAR" on page 493.
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 **Additional 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 **Additional 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. 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. If you choose to replicate logs, be sure that you have sufficient disk space for the additional logs on all the replication partners.

See "How to install a second site for replication" on page 748.

To view the logs from another site

1. Open a web browser.
2. Type the following in the address text box as follows:

   http://*SEPMServer*:9090

   Where *SEPMServer* is the server name or the IP address.

   The IP address can be either IPv4 or IPv6. You must enclose the IPv6 address with square brackets: **http://[*SEPMServer*]:9090**

   The console then downloads. The computer from which you log on must have the Java 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://*SEPMServer*:8443
5. Click **Log On**.

Chapter 29

Managing notifications

This chapter includes the following topics:

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 29-1 lists the tasks you can perform to manage notifications.

Table 29-1 Notification management

Task	Description
Learn about notifications	Learn how notifications work. See "How notifications work" on page 662.
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 668.
Review preconfigured notifications	Review the preconfigured notifications provided by Symantec Endpoint Protection. See "What are the types of notifications and when are they sent?" on page 663.
View unacknowledged notifications	View and respond to unacknowledged notifications. See "Viewing and acknowledging notifications" on page 669.
Configure new notifications	Optionally create notifications to remind you and other administrators about important issues. See "Setting up administrator notifications" on page 671. See "About turning on notifications for remote clients" on page 274.
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 670.

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 trial 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 that 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 damper period of one hour for that notification condition, the server sends only one notification email each hour during the attack.

Note: If you set the **Damper** period to **None** for notifications about critical events, you should make sure that clients can upload critical events immediately. The **Let clients upload critical events immediately** option is enabled by default and configured in the **Communications Settings** dialog box.

See "Managing notifications" on page 661.

See "Establishing communication between the management server and email servers" on page 668.

See "What are the types of notifications and when are they sent?" on page 663.

See "Setting up administrator notifications" on page 671.

See "Viewing and acknowledging notifications" on page 669.

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 661.

See "How upgrades from another version affect notification conditions" on page 672.

Table 29-2 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 29-2 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 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
Client security alert	This notification triggers upon any of the following security events: ■ Compliance events ■ Network and Host Exploit Mitigation 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. **Note:** If you set the notification damper period to **None**, you should make sure that clients can upload critical events immediately. The **Let clients upload critical events immediately** option is enabled by default and configured in the **Communications Settings** dialog box.
Deception Detection	When an attacker attempts to touch or modify a deceptor, the Deception tools log an event. A notification is triggered when: ■ An attacker gets past the client's defenses. ■ An attacker retrieves information about the client computer. ■ An attacker attempts to use the client computer in additional attacks within the enterprise network.
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.

Table 29-2 Preconfigured notifications *(continued)*

Notification	Description
File reputation lookup alert	Alerts the administrators when a file is submitted to Symantec for a reputation check. SONAR and Download Insight use file reputation lookups and submit files to Symantec automatically. The **File Reputation Detection** notification is enabled by default.
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.
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. **Over-deployment** This notification alerts administrators and, optionally, partners, about over-deployed paid licenses. This notification is enabled by default. **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.
Memory Exploit Mitigation Detection	This notification triggers when a Windows vulnerability attack is detected.
Network load alert: requests for virus and spyware full definitions	Alerts the administrators when too many clients request a full definition set, and to potential network bandwidth issues. This notification is enabled by default.
New learned application	This notification triggers when application learning detects a new application.

Table 29-2 Preconfigured notifications *(continued)*

Notification	Description
New risk detected	This notification triggers whenever virus and spyware scans detect a new risk. **Note:** If you set the notification damper period to **None**, you should make sure that clients can upload critical events immediately. The **Let clients upload critical events immediately** option is enabled by default and configured in the **Communications Settings** dialog box.
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. ■ LiveUpdate has new security definitions or engine content. You can specify whether the notification is triggered only by new security definitions, only by new client packages, or by both. This notification is enabled by default.
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.
Power Eraser recommended	Alerts the administrators when a regular scan cannot repair an infection, so the administrators can use Power Eraser. This notification is enabled by default.
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. **Note:** If you set the notification damper period to **None**, you should make sure that clients can upload critical events immediately. The **Let clients upload critical events immediately** option is enabled by default and configured in the **Communications Settings** dialog box.

Table 29-2 Preconfigured notifications *(continued)*

Notification	Description
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. **Note:** If you set the notification damper period to **None**, you should make sure that clients can upload critical events immediately. The **Let clients upload critical events immediately** option is enabled by default and configured in the **Communications Settings** dialog box.
SONAR definitions 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 management server activities, replication failures, backups, and system errors.
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. This notification appears only after an 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 "What are the types of notifications and when are they sent?" on page 663.

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 661.

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**.

See Sending test email messages fails in Endpoint Protection Manager console.

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 661.

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 670.
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 669.

   See "To view all notifications" on page 669.
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 669.

See "Managing notifications" on page 661.

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 **Additional 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 a notification triggers, it 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 a mail server to communicate with the management server.

See "Establishing communication between the management server and email servers" on page 668.

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 let you specify what type of scan triggers the notification.
- Specify actions.
  All notification types provide actions you can specify.

Note: If you set the **Damper** period to **None** for notifications about critical events, you should make sure that clients can upload critical events immediately. The relevant notifications include the following: **Client security alert**, **Single risk event**, **New risk detected**, and **Risk outbreak**. The **Let clients upload critical events immediately** option is enabled by default and configured in the **Communications Settings** dialog box.

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.
- Under **What filter settings would you like to use**, if it is present, specify the filter settings for the notification condition.
- Under **What settings would you like for this notification**, specify the conditions that trigger the notification.
- Under **What should happen when this notification is triggered**, specify the actions that are taken when the notification is triggered.

5 Click **OK**.

See "Managing notifications" on page 661.

See "Viewing and acknowledging notifications" on page 669.

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 663.

Section 7

Protecting clients in virtual environments

Chapter 30

Overview of Symantec Endpoint Protection and virtual infrastructures

This chapter includes the following topics:

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 30-1 Virtual infrastructure features and their use

Feature and use	Description
Use 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 network-based Shared Insight Cache Virtual clients that use any kind of virtual infrastructure can use a network-based Shared Insight Cache to reduce scan loads. **Note:** As of 14.0, a vShield-enabled Shared Insight Cache is no longer supported. See "About Shared Insight Cache" on page 677. See "What do I need to do to use a network-based Shared Insight Cache?" on page 678.
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. The Virtual Image Exception tool runs in a virtual environment only. See "About the Virtual Image Exception tool" on page 677.
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 "Using Symantec Endpoint Protection in non-persistent virtual desktop infrastructures" on page 694. See "Purging obsolete non-persistent VDI clients to free up licenses" on page 696.

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 678.

See “Customizing Shared Insight Cache settings” on page 682.

See “Using Symantec Endpoint Protection in virtual infrastructures” on page 675.

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 690.

See “Using Symantec Endpoint Protection in virtual infrastructures” on page 675.

Chapter 31

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 31-1 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 679. See "Installing and uninstalling a network-based Shared Insight Cache" on page 680.
Step 2: In the Virus and Spyware policy in Symantec Endpoint Protection Manager, enable your virtual clients to use Shared Insight Cache	See "Enabling the use of a network-based Shared Insight Cache" on page 682.

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 Shared Insight Cache settings" on page 682.
- View related events in the log.
  See "Viewing network-based Shared Insight Cache log events" on page 686.
- Use the Windows Performance Manager to monitor its performance.
  See "Monitoring network-based Shared Insight Cache performance counters" on page 688.

System requirements for implementing a network-based Shared Insight Cache

The network-based Shared Insight Cache server is designed to run on a standalone physical or virtual machine. Shared Insight Cache should not be installed to a system running other database applications or high-availability server applications, such as Symantec Endpoint Protection Manager or Microsoft SQL Server.

Table 31-2 describes the minimum system requirements that a virtual infrastructure needs to run Shared Insight Cache.

Table 31-2 Network-based Shared Insight Cache system requirements

Requirement	Description
Software	■ Windows Server 2008 and later ■ Windows Server 2012 and Windows Server 2012 R2 ■ Windows Server 2016 ■ Windows Server 2019 ■ .NET Framework 4

Table 31-2 Network-based Shared Insight Cache system requirements *(continued)*

Requirement	Description
CPU	Shared Insight Cache must be installed on a dedicated server or a virtual machine.
Memory	2 GB minimum
Available disk space	100 MB minimum

See "About Shared Insight Cache" on page 677.

See "Installing and uninstalling a network-based Shared Insight Cache" on page 680.

Installing and uninstalling a network-based Shared Insight Cache

Before you install the network-based Shared Insight Cache, ensure that you have met all the system requirements and that you are logged on as a Windows administrator. You install and run the Shared Insight Cache on a standalone physical or virtual machine.

Note: You should not use DBCS or high-ASCII characters in the host name of the server on which you install a Shared Insight Cache. You should also refrain from using DBCS or high-ASCII characters in the user name that you use to access it. These characters cause the Shared Insight Cache service to fail to start.

See "System requirements for implementing a network-based Shared Insight Cache" on page 679.

To install a network-based Shared Insight Cache

1. On the Symantec Endpoint Protection installation file, navigate to the `Tools/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 about the server.

7 Click **Install**.

8 When the installation has completed, click **Finish**.

See "Customizing Shared Insight Cache settings" on page 682.

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 686.

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 the use of a network-based Shared Insight Cache

For communication with Symantec Endpoint Protection clients over the network, by default Shared Insight Cache uses no authentication and no SSL. 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.

See "Customizing Shared Insight Cache settings" on page 682.

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. On the **Shared Insight Cache** tab, check **Shared Insight Cache using Network**.
3. Click **Require SSL** if you enabled SSL authentication in the configuration file.
4. In the **Hostname** box, type the host name of the host on which you installed Shared Insight Cache.
5. In the **Port** box, type the port number of Shared Insight Cache.
6. Optionally, if you configured authentication for Shared Insight Cache:
   - In the **Username** box, type the user name.
   - Optionally, click **Change Password** to change the default password (null) to the password that you created for authentication.
     Leave these fields empty if you do not want to use a password.
7. Click **OK**.

See "What do I need to do to use a network-based Shared Insight Cache?" on page 678.

Customizing Shared Insight Cache 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, see:

Configuration Editor Tool (SvcConfigEditor.exe)

Table 31-3 describes the options that you can configure.

Table 31-3 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. The listening port is used by clients to submit scan results for files and to make requests to determine if the client should scan a file. If the range for the port 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 Netsh.exe. 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 Server 2008. For more information, see: Configuring HTTP and HTTPS
Status Service Listening Port The default value is 9006.	Port the server uses to communicate status about the server. The status listening port uses a SOAP-based interface on the port specified in the configuration section. This interface provides a mechanism by which an administrator can query information and status about the Cache Server. 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 31-3 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 686.
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 31-3 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 the use of a network-based Shared Insight Cache" on page 682.

To customize Shared Insight Cache settings

1 Navigate to and open the following file:

```
C:\Program Files (x86)\Symantec\Shared Insight
Cache\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 686.

See "What do I need to do to use a network-based Shared Insight Cache?" on page 678.

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 689.

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 31-4 describes the levels that you can set.

Table 31-4 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 Shared Insight Cache settings" on page 682.

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 31-5 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 689.

See "What do I need to do to use a network-based Shared Insight Cache?" on page 678.

Troubleshooting issues with Shared Insight Cache

Table 31-6 provides suggestions for how to troubleshoot issues with Shared Insight Cache.

Table 31-6 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 686.
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 686.

See "Monitoring network-based Shared Insight Cache performance counters" on page 688.

Chapter 32

Using Virtual Image Exception

This chapter includes the following topics:

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 32-1 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 "Specifying when repaired files, backup files, and quarantined files are automatically deleted" on page 454.
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 455.
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 692. See vietool on page 847.
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 692.
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 691.

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.

Warning: The client must be the same version as the Virtual Image Exception tool.

For the most up-to-date information about requirements and supported platforms, see the following Web page:

Release notes, new fixes, and system requirements for all versions of Endpoint Protection

See "Using the Virtual Image Exception tool on a base image" on page 690.

Running the Virtual Image Exception tool

Before you run the Virtual Image Exception tool, ensure that you have met all of the system requirements.

Warning: The client must be the same version as the Virtual Image Exception tool.

See "System requirements for the Virtual Image Exception tool" on page 691.

To run the Virtual Image Exception tool

1. From the Symantec Endpoint Protection Tools folder of the installation file, 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 847.

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 690.

Chapter 33

Non-persistent virtual desktop infrastructures

This chapter includes the following topics:

Using Symantec Endpoint Protection in non-persistent virtual desktop infrastructures

Table 33-1 Tasks to use Symantec Endpoint Protection in non-persistent virtual desktop infrastructures

Step	Description
Step 1: Set up the base image.	You configure the Symantec Endpoint Protection client in your base image to indicate that it is a non-persistent virtual client. See "Setting up the base image for non-persistent guest virtual machines in VDIs" on page 695.
Step 2: In Symantec Endpoint Protection Manager, configure a separate purge interval for offline non-persistent VDI clients.	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. See "Purging obsolete non-persistent VDI clients to free up licenses" on page 696.

Setting up the base image for non-persistent guest virtual machines in VDIs

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 33-2 Tasks to set up the base image for non-persistent GVMs

Step	Description
Step 1: Install Symantec Endpoint Protection on the base image.	See "Choosing a method to install the client using the Client Deployment Wizard" on page 119.
Step 2: Disable Tamper Protection in the management server so that you can modify the registry.	See "Changing Tamper Protection settings" on page 501.
Step 3: Make sure that Symantec Endpoint Protection Manager correctly counts the number of licenses for non-persistent virtual clients.	The advantage of non-persistent clients is that offline non-persistent clients do not count toward the number of deployed licenses. Only online clients count. To mark a virtual client as a non-persistent client, you must create a registry key in the base image. See "How to manage the license count for non-persistent VDI clients" on page 695.
Step 4: In Symantec Endpoint Protection Manager, re-enable Tamper Protection.	See "Changing Tamper Protection settings" on page 501.

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 "Purging obsolete non-persistent VDI clients to free up licenses" on page 696.

How to manage the license count for non-persistent VDI clients

The management server counts each license for clients on physical computers, whether the computer is online or offline. For virtual clients, the management server counts the licenses of online non-persistent clients only. Offline non-persistent clients do not count. Make your virtual clients non-persistent if you have more users than you have clients.

To mark a virtual client as a non-persistent client, you must create a registry key in the base image.

To manage the license count for non-persistent VDI clients

1. After you have installed the Symantec Endpoint Protection client and disabled Tamper Protection, open the registry editor on the base image.

   See "Changing Tamper Protection settings" on page 501.

2. Navigate to one of the following registry keys:
   - On 32-bit systems: HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\SMC\
   - On 64-bit systems: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Symantec\Symantec Endpoint Protection\SMC\
3. Create a new subkey named **Virtualization**.
4. In the **Virtualization** subkey, create a key of type DWORD named **IsNPVDIClient** and assign it a value of 1.

See "Purging obsolete non-persistent VDI clients to free up licenses" on page 696.

See "Setting up the base image for non-persistent guest virtual machines in VDIs" on page 695.

Purging obsolete non-persistent VDI clients to free up licenses

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 virtual clients are purged at the same interval that obsolete physical clients are purged.

Online non-persistent clients count toward the number of deployed licenses; offline non-persistent clients do not.

See "How to manage the license count for non-persistent VDI clients" on page 695.

You can also filter the offline non-persistent clients out of the view on the **Clients** page.

To purge obsolete non-persistent VDI clients to free up licenses

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** check box 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 694.

Section 8

Configuring and managing the management server

Chapter 34

Configuring the connection between the management server and the clients

This chapter includes the following topics:

Setting up HTTPS communications between a Symantec Endpoint Protection Manager and the clients

Symantec Endpoint Protection Manager uses an Apache web server to communicate with clients and provide reporting services. For new installations of Symantec Endpoint Protection 14, HTTPS communications are enabled by default. HTTPS is a secure protocol that uses a certificate to sign and encrypt data, which provides for the confidentiality and the integrity of the communications.

The web server in version 12.1 uses the unencrypted protocol HTTP for all communications by default. If you upgrade to Symantec Endpoint Protection 14 from version 12.1, the Symantec Endpoint Protection Manager retains the settings during the upgrade. If you had not enabled

HTTPS in version 12.1, you can configure the Symantec Endpoint Protection Manager Apache web server to use an HTTPS connection after the upgrade.

Table 34-1 Configuring HTTPS communication to the client

Step	Description
Step 1: Check that the default HTTPS port is available	By default, HTTPS traffic uses port 443. In some networks, port 443 may already be bound to another application or service. Before you enable HTTPS communication, you must check to see if the default port is available. See "Verifying port availability" on page 700.
Step 2: Change the default HTTPS port as needed	If port 443 is not available, choose an unused port from the high port range (49152-65535). Configure the management server to use the new port. Update the management server list to reflect the new port. See "Changing the HTTPS port for Apache for client communication" on page 701. See "Configuring a management server list for load balancing" on page 736.
Step 3: Enable HTTPS communication to the client	Edit the Apache httpd.conf file to allow HTTPS communication to the client. Test the connection, and then switch the clients to HTTPS communication. See "Enabling HTTPS client-server communications" on page 702.

See "Managing the client-server connection" on page 161.

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 another application or service does not use the new port.

To verify port availability

- Open a command prompt and enter the following case-sensitive command:

  ```
  netstat -an | find ":port" | find "LISTENING"
  ```

  Where *port* represents the port number for which you want to check availability. For example, to see if port 443 is available, enter:

  ```
  netstat -an | find ":443" | find "LISTENING"
  ```

  If the `netstat` command returns a result, you must find an unused port. You use the same command, but replace *port* with the port of your choice. If this command yields no results, then the port is free to use.

See "Changing the HTTPS port for Apache for client communication" on page 701.

See "Setting up HTTPS communications between a Symantec Endpoint Protection Manager and the clients" on page 699.

Changing the HTTPS port for Apache for client communication

The default HTTPS port for Apache is port 443. If Symantec Endpoint Protection Manager hosts other HTTPS websites, port 443 may already be assigned to one of these websites. You should use a different port for new installations to minimize conflict with any applications that already use the default port 443. If you want clients to use the default port to communicate with Symantec Endpoint Protection Manager, you should first verify that port is available.

Note: If you customize the HTTPS port number after you deploy the client software, the clients lose communication with the management server. They reestablish communication after the next client update from the server, which contains the new connection information. You can also use a Communication Update Package.

Restoring client-server communications with Communication Update Package Deployment

---

After you complete this procedure, you enable HTTPS client-server communications.

To change the HTTPS port for Apache for client communication

1. In a text editor, open the following file:

   SEPM_Install\apache\conf\ssl\sslForClients.conf

   SEPM_Install by default is C:\Program Files\Symantec\Symantec Endpoint Protection Manager.

   Note: The enclosing folder *SEPM_Install*\apache\conf\ssl\ may be read-only. In that case, you may need to uncheck **Read-only** in the folder properties.

   ---

2. Edit the following lines and replace the default of 443 with the new port number:

   ```
   Listen 443
   ```

   ```
   <VirtualHost _default_: 443>
   ```

3. Save the file and close the text editor.

See "Verifying port availability" on page 700.

See "Enabling HTTPS client-server communications" on page 702.

See "Setting up HTTPS communications between a Symantec Endpoint Protection Manager and the clients" on page 699.

Enabling HTTPS client-server communications

You edit the httpd.conf file to enable secure communication between the Symantec Endpoint Protection Manager server and the clients using the HTTPS protocol.

If you need to use an alternate port for secure communication, you must change the port assignment in Symantec Endpoint Protection Manager first.

For new installations of Symantec Endpoint Protection 14.x, HTTPS client-server communications is enabled by default. If you upgrade to version 14.x from a version of 12.1, then the settings for client-server communication carry over. HTTPS client-server communications is not enabled by default for version 12.1.x.

To enable HTTPS for the Apache web server

1. In a text editor, open the following file:

   SEPM_Install\apache\conf\httpd.conf

   SEPM_Install by default is C:\Program Files\Symantec\Symantec Endpoint Protection Manager.

2. Find the following text string and remove the hash mark (#):

   ```
   #Include conf/ssl/sslForClients.conf
   ```

3. Save and then close the file.

4. Restart the **Symantec Endpoint Protection Manager Webserver** service.

   Stopping and restarting the Symantec Endpoint Protection Manager Webserver service also stops and restarts the Symantec Endpoint Protection Manager service.

   See “Stopping and starting the Apache Web server” on page 769.

To verify HTTPS works correctly

1. Enter the following URL in a web browser:

   https://*SEPMServer*:*port*/secars/secars.dll?hello,secars

   Where *SEPMServer* is the server host name for Symantec Endpoint Protection Manager and *port* is the HTTPS port number. By default, HTTPS traffic uses port 443.

2. If the browser displays the word **OK**, the HTTPS connection is successful.

   If a page error displays, repeat the previous steps and check that you formatted all strings correctly. Also check that you entered the URL correctly.

   If you did not update the management server with a certificate authority-signed certificate and private key pair, the web browser displays a warning that the certificate is not trusted. The same warning appears when you access the website from a URL that is different than the subject name on the management server certificate, which is expected.

To switch the clients to use HTTPS for communication with Symantec Endpoint Protection Manager

1. In the Symantec Endpoint Protection Manager console, on the **Policies** tab, click **Policy Components > Management Server Lists**.
2. Double-click the management server list that your client groups and locations use. If you only have the default management server list, duplicate it, and then double-click the new list to edit it.

   You can also click **Add a Management Server List**, under **Tasks**. Add the server information under **Management Servers**, **Add > New Server**. You can add one **New Server** entry for server IP address, and one for server name.

   See "Copying and pasting a policy on the Policies page" on page 319.
3. Click **Use HTTPS protocol**.

   Only click **Verify certificate when using HTTPS protocol** if you have previously updated the management server with a Certificate Authority-signed certificate and a private key pair.

   See "Best practices for updating server certificates and maintaining the client-server connection" on page 707.

   Note: If you used a custom HTTPS port number in the `sslForClients.conf` file, edit the server from the list of management servers. Click **Customize HTTPS port**, and then edit the port to match the number you previously used.

   Click **OK** to save the custom port.

   ---
4. Click **OK** to save your management server list.
5. If you edited a copy of the default management server list, right-click it, click **Assign**, and then assign it to every group and location.

   See "Assigning a management server list to a group and location" on page 737.

As the clients receive the updated management server list, the clients switch to HTTPS for communication with Symantec Endpoint Protection Manager. The change on the client side can take up to three heartbeat intervals to complete.

Confirm client communication to the management server

1. On the Symantec Endpoint Protection client, click **Help > Troubleshooting > Server Connection Status**.
2. Under **Last Attempted Connection** and **Last Successful Connection**, confirm the display of both the server address and the port number for HTTPS communications.
3. Click **Connect Now** to force an immediate connection, if desired.

See "Changing the HTTPS port for Apache for client communication" on page 701.

See "Setting up HTTPS communications between a Symantec Endpoint Protection Manager and the clients" on page 699.

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 34-2 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 "Updating policies and content on the client using push mode or pull mode" on page 165. For more information about setting heartbeat intervals, see the Symantec Endpoint Sizing and Scalability Best Practices white paper.

Table 34-2 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 for load balancing" on page 736. ■ 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 215. See "Using third-party distribution tools to update client computers" on page 225. ■ Randomize the time when LiveUpdate downloads content to the client computers. See "Randomizing content downloads from a LiveUpdate server" on page 207. See "Randomizing content downloads from the default management server or a Group Update Provider" on page 206. ■ Download content updates when users are not actively using the client computer. See "Configuring Windows client updates to run when client computers are idle" on page 208.
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 437. See "Customizing Auto-Protect for Windows clients" on page 468.

Table 34-2 Tasks to improve performance on the server and on the client *(continued)*

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 728. ■ Specify how many log entries the client computer can keep in the database, and how long to keep them. See "Specifying the log size and how long to keep log entries in the database" on page 729. ■ Filter the less important risk events and system events out so that less data is forwarded to the server. See "Modifying log handling and notification settings on Windows computers" on page 478. ■ Reduce the number of clients that each management server manages. See "Configuring a management server list for load balancing" on page 736. See "Installing Symantec Endpoint Protection Manager" on page 43. ■ Reduce the heartbeat frequency, which controls how often the client logs are uploaded to the server See "Updating policies and content on the client using push mode or pull mode" on page 165. ■ 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 730.
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 724.

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 707.

See "Update the server certificate on the management server without breaking communications with the client" on page 709.

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 755.

See "Updating or restoring a server certificate" on page 711.

See "Generating a new server certificate" on page 758.

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:
  `SEPM_Install\Server Private Key Backup\recovery_timestamp.zip`
  SEPM_Install by default is C:\Program Files\Symantec\Symantec Endpoint Protection Manager.
  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 34-3 lists the steps to update the certificate without orphaning the clients that the server manages.

Table 34-3 Steps to update server certificates

Step	Description
Step 1: Break the replication relationship*	If the management server you want to update replicates with other management servers, break the replication relationship. See "Disabling replication and restoring replication before and after an upgrade" on page 153.
Step 2: 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 "Update the server certificate on the management server without breaking communications with the client" on page 709.
Step 3: 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 168.

Table 34-3 Steps to update server certificates *(continued)*

Step	Description
Step 4: Update the server certificate	Update the server certificate. If you also plan to upgrade the management server, upgrade the certificate first. See "Upgrading a management server" on page 149. See "Updating or restoring a server certificate" on page 711. You must restart the following services to use the new certificate: ■ The Symantec Endpoint Protection Manager service ■ The Symantec Endpoint Protection Manager Webserver service ■ The Symantec Endpoint Protection Manager API service
Step 5: Enable server certificate verification again	Enable secure communications between the server and the clients again. See "Update the server certificate on the management server without breaking communications with the client" on page 709.
Step 6: Wait for all clients to receive the updated policy	The client computers must receive the policy changes from the previous step.
Step 7: Restore the replication relationship*	If the management server you updated replicates with other management servers, restore the replication relationship. See "Disabling replication and restoring replication before and after an upgrade" on page 153.

* You only need to perform these steps if you use replication in your Symantec Endpoint Protection Manager environment.

See "Installing Symantec Endpoint Protection Manager" on page 43.

See "Generating a new server certificate" on page 758.

Update the server certificate on the management server without breaking communications with the client

Symantec Endpoint Protection Manager uses a certificate to authenticate communications between it and the Symantec Endpoint Protection clients. The certificate also digitally signs the policy files and installation packages that the client downloads from it. The clients store a cached copy of the certificate in the management server list. 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, but do not authenticate communications from the management server.

You disable secure communications to update the certificate in the following situations:

- A site with a single Symantec Endpoint Protection Manager
- A site with more than one Symantec Endpoint Protection Manager, if you cannot enable failover or load balancing

---

Note: If the certificate is corrupted but otherwise still valid, you can perform disaster recovery as a best practice.

See "Disaster recovery best practices" on page 752.

After you update the certificate and the clients check in and receive it, enable secure communications again.

When you update the certificate on a site with multiple management servers and use failover or load balancing, the certificate updates on the management server list. During the process of failover or load balancing, the client receives the updated management server list and the new certificate.

To update the server certificate on a single management server site without breaking communications with the client

1. On the console, click **Policies > Policy Components > Management Server Lists**.
2. Under **Tasks**, click **Copy the List**, and then click **Paste List**.
3. Double-click the copy of the list to edit it, and then make the following changes:
   - Click **Use HTTP protocol**.
   - For each server address under **Management Servers**, click **Edit**, and then click **Customize HTTP port**.
     Leave it at the default of 8014. If you use a custom port, use it here.
4. Click **OK**, and then click **OK** again.
5. Right-click the copy of the list, and then click **Assign**.
6. On the console, click **Clients > Policies > General Settings**.
7. On the **Security Settings** tab, uncheck **Enable secure communications between the management server and clients by using digital certificates for authentication**, and then click **OK**.
8. Wait at least three heartbeat cycles after making this change on all groups before you move to step 9.

   Make sure that you also configure this setting for the groups that do not inherit from a parent group.

9 Update the server certificate.

See "Updating or restoring a server certificate" on page 711.

10 Click **OK**.

To reenable the original settings, wait at least three heartbeat cycles, recheck **Enable secure communications between the management server and clients by using digital certificates for authentication**, and then reassign the original management server list back to your groups.

To update the server certificate on a multi-management server site without breaking communications with the client

1 On the console, ensure that your clients are configured to load balance or failover to at least one other Symantec Endpoint Protection Manager.

See "Setting up failover and load balancing" on page 732.

If you cannot enable load balancing or failover, use the single management server site procedure to first disable then reenable secure communications.

2 Update the server certificate on Symantec Endpoint Protection Manager.

See "Updating or restoring a server certificate" on page 711.

3 Wait at least three heartbeat cycles, and then update the server certificate on the next Symantec Endpoint Protection Manager on the site.

4 Repeat steps 2 and 3 until each Symantec Endpoint Protection Manager on the site has the new certificate.

Note: Users who are out of the office or on leave may not receive these updates on their device because it is offline. Many institutions run the failover method for 30 days or more to catch as many out-of-office clients as possible. You may want to leave one Symantec Endpoint Protection Manager running for 90 days with the old certificate to ensure that those users are not orphaned.

See "About server certificates" on page 706.

See "Best practices for updating server certificates and maintaining the client-server connection" on page 707.

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 43.
- 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 706.

See "Best practices for updating server certificates and maintaining the client-server connection" on page 707.

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 "Update the server certificate on the management server without breaking communications with the client" on page 709.
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 `SEPM_Install\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.

   SEPM_Install by default is C:\Program Files\Symantec\Symantec Endpoint Protection Manager.
7. You must restart the following services to use the new certificate:
   - The Symantec Endpoint Protection Manager service
   - The Symantec Endpoint Protection Manager Webserver service
   - The Symantec Endpoint Protection Manager API service

See “Stopping and starting the management server service” on page 151.

See “Stopping and starting the Apache Web server” on page 769.

Chapter 35

Configuring the management server

This chapter includes the following topics:

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 35-1 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 716.
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 302.

Table 35-1 Server management *(continued)*

Task	Description
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 756.
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 668.
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 239.
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 200.
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 717.
Manage server certificates	The Symantec Endpoint Protection Manager server uses a server certificate to encrypt data for the communication between all servers, and clients 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 706. See "Updating or restoring a server certificate" on page 711. See "Backing up a server certificate" on page 755. See "Generating a new server certificate" on page 758.

Table 35-1 Server management *(continued)*

Task	Description
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 "Using RSA SecurID authentication with Symantec Endpoint Protection Manager" on page 285.
Configure two-factor authentication for Symantec Endpoint Protection Manager with Symantec VIP	If you use Symantec VIP in your environment for two-factor authentication, you can enable it for those administrators who authenticate with Symantec Endpoint Protection Manager Authentication. See "Configuring two-factor authentication with Symantec VIP" on page 288.
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 "How to install a second site for replication" on page 748. ■ Install the management server on another computer using the recovery file. See "Reinstalling or reconfiguring Symantec Endpoint Protection Manager" on page 756.
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 151.

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 739.

- 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 732.
- 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 719.
- Replication partner
  A relationship created between two sites to enable data replication between them.
  See "Setting up sites and replication" on page 739.

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.

See "Managing Symantec Endpoint Protection Manager servers and third-party servers" on page 714.

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**.

Chapter 36

Managing databases

This chapter includes the following topics:

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 36-1 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 754. See "Scheduling automatic database backups" on page 723. See "Disaster recovery best practices" on page 752. 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 731.
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 724.
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 725.

Table 36-1 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 "Downloading content from LiveUpdate to the Symantec Endpoint Protection Manager" on page 186. See "Reverting to an older version of the Symantec Endpoint Protection security updates" on page 213. ■ 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, Symantec Endpoint Protection Sizing and Scalability Best Practices White Paper.

Table 36-1 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 728. ■ Specify how many log entries the client computer can keep in the database, and how long to keep them. See "Specifying the log size and how long to keep log entries in the database" on page 729. ■ Filter the less important risk events and system events out so that less data is forwarded to the server. See "Modifying log handling and notification settings on Windows computers" on page 478. ■ 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 730. ■ Reduce the number of clients that each management server manages. See "Configuring a management server list for load balancing" on page 736. ■ Reduce the heartbeat frequency, which controls how often the client logs are uploaded to the server. See "Updating policies and content on the client using push mode or pull mode" on page 165.
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 727. See "Exporting data to a Syslog server" on page 726.
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 "Choosing which security features to install on the client" on page 121.

Table 36-1 Database management tasks *(continued)*

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 215. To reduce disk space and database size, you can reduce the number of content revisions that are kept on the server. See "Downloading content from LiveUpdate to the Symantec Endpoint Protection Manager" on page 186.
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 759.

See "Verifying the connection with the database" on page 774.

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

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 754.

To schedule automatic database backups

1. In the console, click **Admin** > **Servers**.
2. Under **Servers**, click **Local Site (My Site)** > **localhost**.
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.

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 723.

Increasing the Microsoft SQL Server database file size

If you use the 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 SQL Server database holds.

See "Scheduling automatic database maintenance tasks" on page 724.

To increase the Microsoft SQL Server database size

1. On the Microsoft SQL server computer, open the SQL Server Management Studio.
2. In the Object Explorer, Expand the "Databases" 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 727.

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. By default, that folder path is C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\data\dump. Entries are placed in a .tmp file until the records are transferred to the text file.

Note: You cannot restore the database by using exported log data.

Table 36-2 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 36-2 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

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**.

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 log entries that are kept, and the number of days that each entry is kept on the client.

You can configure whether to upload each type of client log to the server. You can also configure the maximum upload size. If you choose not to upload the client logs, you cannot perform the following tasks:

- 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 the log size and how long to keep log entries in the database" on page 729.

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 and Host Exploit Mitigation** events are aggregated.
6. Click **OK**.

Specifying the log size and 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 728.

To specify the log size and 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 default location:

`C:\Program Files (x86)\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 36-3 lists the Windows registry keys and their default values and describes what they do.

Table 36-3 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.
`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 719.

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 754.

See "Specifying the log size and how long to keep log entries in the database" on page 729.

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.

Chapter 37

Managing failover and load balancing

This chapter includes the following topics:

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 using a management server list

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.

Table 37-1 lists the tasks that you should perform to set up failover and load balancing.

Table 37-1 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 management servers for failover and load balancing. See "About failover and load balancing" on page 733.
Install additional management servers.	See "Installing a management server for failover or load balancing" on page 735. The number of clients for each management server depends on several factors, such as the log sizes. To calculate how many management servers you need, see: Symantec Endpoint Protection Sizing and Scalability Best Practices White Paper
Add management servers to a management server list.	To set up load balancing, you add multiple 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 can connect. See "Configuring a management server list for load balancing" on page 736.
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 737.

See "Setting up sites and replication" on page 739.

If the management server goes offline, or the client and the management server do not communicate, you should also troubleshoot the problem.

See "Troubleshooting connectivity problems between Symantec Endpoint Protection Manager and the Symantec Endpoint Protection client" on page 765.

About failover and load balancing

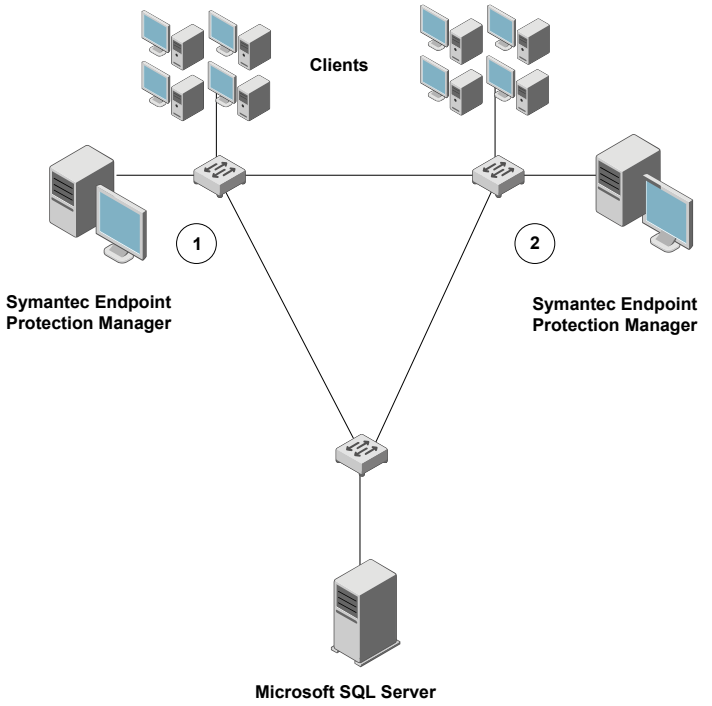
You can install two or more management servers that communicate with one Microsoft SQL Server database and configure them for failover or load balancing. Since you can install only one Symantec Endpoint Protection Manager to communicate with the embedded database, you can set up failover only if you 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.

Load balancing occurs with 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 37-1 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 37-1 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 "Setting up failover and load balancing" on page 732.

See "Configuring a management server list for load balancing" on page 736.

See "Determining how many sites you need" on page 746.

See "Setting up sites and replication" on page 739.

Installing a management server for failover or load balancing

Failover configurations are used to maintain communication when clients cannot communicate with a Symantec Endpoint Protection Manager. Load balancing is used to distribute client management between management servers. You can configure failover and load balancing by assigning priorities to management servers in management server lists.

Failover and load balancing installations are supported only when the original Symantec Endpoint Protection Manager uses a Microsoft SQL Server database. The SQL Server Native Client files also must be installed on the computer that you use for failover or load balancing. You do not install servers for failover or load balancing when the site is configured to use the embedded database.

To install a management server for failover or load balancing

1. Install a Symantec Endpoint Protection Manager.

   See "Installing Symantec Endpoint Protection Manager" on page 43.

2. In the **Management Server Configuration Wizard** panel, check **Custom Configuration**, and then click **Next**.

   See "Configuring Symantec Endpoint Protection Manager after installation" on page 44.

3. Select the number of clients you expect the server to manage, and then click **Next**.
4. Check **Install an additional management server to an existing site**, and then click **Next**.
5. In the server information panel, accept or change the default values, and then click **Next**.
6. In the **Microsoft SQL Server Information** dialog box, click **OK** in the message about installing the SQL Server client tools.

7 Enter the remote server values for the following text boxes:

Step One tells the Symantec Endpoint Protection Manager where to find the SQL Server on the network, which includes host name, instance name, and port.

You also pick the authentication type, including Windows Authentication or SQL authentication.

- **Database server***instance_name*
  SQL server port
  Database name
  SQL client folder (on the local computer)
  If this text box does not automatically populate with the correct path, the Microsoft SQL Client Utility is not installed or it is not installed correctly.

8 **Step Two** tells the Symantec Endpoint Protection Manager how to authenticate to the SQL Server and includes the database name, database user, and database user's password.

You should have had this information available already for when you installed the first management server for that site.

9 Click **Next**.

10 Specify and confirm a password for the Symantec Endpoint Protection Manager admin account.

Optionally, provide an administrator email address.

11 Click **Next**.

12 At the warning, read the text message, and then click **OK**.

13 In **Management Server Completed** panel, click **Finish**.

Configuring a management server list for load balancing

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. You can only configure load balancing when a site includes more than one management server.

Load balancing occurs between the servers that are assigned to priority 1 in a management server list. If more than one server is assigned to priority 1, the clients randomly choose one of the servers and establish communication with it. If all priority 1 servers fail, clients connect with the server assigned to priority 2.

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 733.

To configure a management server list for load balancing

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.

   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 737.

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 for load balancing" on page 736.

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**.

Chapter 38

Managing sites and replication

This chapter includes the following topics:

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 as a single site. Organizations with more than one data center or physical location generally use multiple sites.

Replication configurations are used for redundancy. Data from one database is duplicated, or replicated, on another database. If one database fails, you can still manage and control all clients because the other database contains the client information.

See "What are sites and how does replication work?" on page 741.

Table 38-1 Process for setting up sites and replication

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 multiple sites only in specific circumstances and that you add a maximum of five sites in each site farm. If you do add an additional site, decide which site design works for your organization. See "Deciding whether or not to set up multiple sites and replication" on page 744. See "Determining how many sites you need" on page 746.
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 43.
Step 3: Install Symantec Endpoint Protection Manager on the second site	You create a second site by installing a second management server. The second site is classified as a remote site and the management server is called a replication partner. Replication occurs according to the default schedule that when you added the second site during the initial installation. After you have added a replication partner, you can change the replication schedule and what data is replicated. See "How to install a second site for replication" on page 748. 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. If you upgrade the management server on one site, you must upgrade the management server version on all sites. See "Replicating data immediately" on page 750.
Step 4: Check the history for replication events (optional)	If you need to check that the replication occurred or to troubleshoot the replication events, look at the System log. In the second management server, view the System log. Filter for the **Administrative** > **Replication events** event type. See "Viewing logs" on page 655.

You can also reconfigure a management server to replicate the data with a currently existing site in your network. Or, if you have two non-replicating sites, you can convert one of the sites into a site that replicates with the second site.

See "Reinstalling or reconfiguring Symantec Endpoint Protection Manager" on page 756.

- After you configure the Symantec Endpoint Protection, you should back up the database, which contains all your configuration changes.
  See "Backing up the database and logs" on page 754.
- If you disable a replication partner to upgrade to the latest version of the management server, you must re-add the replication partner.
  See "Disabling replication and restoring replication before and after an upgrade" on page 153.
  See "Upgrading to a new release" on page 141.

See "Connecting to a directory server on a replicated site" on page 240.

What are sites and how does replication work?

Sites and replication partners

A site is a Symantec Endpoint Protection Manager database with one or more Symantec Endpoint Protection Managers attached to that database. 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 replication partner is an individual management server within the second site, or remote site. A site may have as many replication partners as needed. Each partner 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.

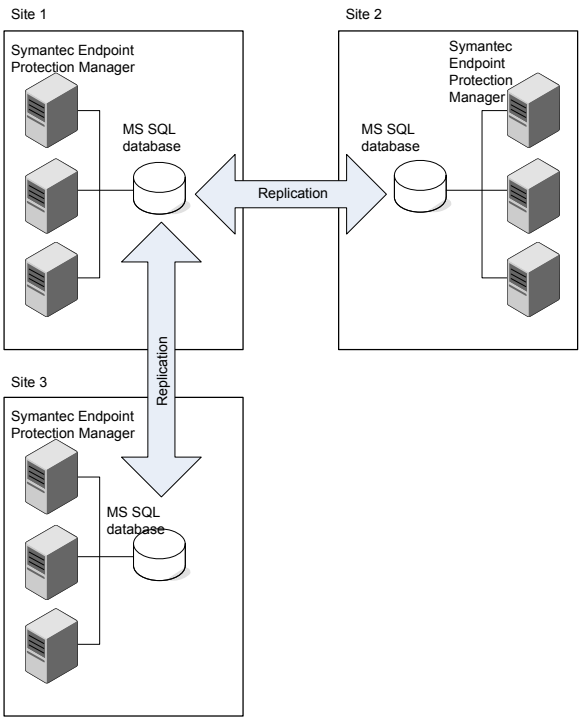
- Site partners share a single Microsoft SQL Server database.

How does replication work?

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.

Figure 38-1 How replication works between the main site and two remote sites



For more information on how often to replicate, see the following article: The Philosophy of SEPM Replication Setup

See "Deciding whether or not to set up multiple sites and replication" on page 744.

See "Determining how many sites you need" on page 746.

See "How to resolve data conflicts between sites during replication" on page 743.

Determining the size of the replication server

A replication partner requires a larger database than a single management server installation. The increased size requirements for the replication server include the following factors:

- Number of managed clients
- Client installation package sizes retained in the database
- Number of log files retained
- Database maintenance settings
- Log size and expiration timeframes
- Definition update sizes
- Database backup information requirements

In general, the hard disk requirements for the replication server should be at least three times the hard disk space used by the original Symantec Endpoint Protection Manager for the initial replication.

See "How to install a second site for replication" on page 748.

Replication considerations and best practices

Symantec Endpoint Protection Sizing and Scalability Best Practices White Paper

How to resolve data conflicts between sites during replication

Replication causes data to be transferred or forwarded to another management server. Sites can have multiple replication partners, and any changes made on one partner are replicated to all sites.

What data is duplicated?

Neither replication site overrides the other. Instead they compare what each site has, and if one site has a package or piece of content the other does not, then it is shared. If all LiveUpdate content and client packages match up, then nothing is exchanged.

The replication partners duplicate the following data:

- Policies and groups (required bidirectional)
- LiveUpdate content and client installation packages, if you specify these options (optional bidirectional)
- Logs (optional bidirectional or unidirectional)

If you upgrade the management server on one site, you must upgrade the management server version on all sites. Replication does not occur if the database schema versions do not match.

Table 38-2 describes how the management server resolves conflicts if administrators change settings on the sites in a site farm.

Table 38-2 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.

Deciding whether or not to set up multiple sites and replication

Before you install a second site, you should decide whether or not multiple sites and replication are a good choice in your network. Setting up more than one site adds a complexity that you may not need. Multiple sites can cause certain tasks such as viewing client logs and reports more difficult. Generally, you should install only one site.

The main purposes to set up multiple sites and replication are:

- If your network has a slow WAN link.
  Multiple sites provide a second management server to which clients in multiple geographical areas can connect locally. For example, suppose a company has several large offices in both Germany and in the United States. If the connection between Germany and the United States is slow, then the company should create one site in Germany and one site in the United States. The Germany clients can connect to the Germany site and the United States clients can connect to the United States site. This distribution reduces the number of clients that have to communicate over the slow WAN link.

- For database redundancy.
  Replication ensures that if one datacenter was corrupted or lost, you would have backed up the database in a different datacenter.

In some situations, you should use a Group Update Provider (GUP) instead of multiple sites and replication. Use a GUP when you have either a lot of clients, or clients that are distributed over several geographical locations.

Note: You should not set up more than five replicated sites.

Table 38-3 Deciding whether to use more than one site with replication, a GUP, or neither

Question	Answer	Use multiple sites with replication or use a GUP
Do you have more than 45,000 clients?	Yes. Do you have either multiple locations or a slow WAN link that connects to a location with more than 1,000 clients?	Yes. ■ For a slow WAN link, consider using replication. ■ For multiple locations, consider using a GUP.
		No. You do not need either replication or a GUP.
	No. Do you have a slow WAN link that connects to a location with more than 1,000 clients?	Yes. Consider using replication.
		No. You do not need either replication or a GUP.
Do you have a slow WAN link?	Yes. Do you have multiple locations with more than 1,000 clients per location?	Yes. Consider using replication.
		No. Consider using a GUP.
	No. Do you have multiple locations with more than 1,000 clients per location?	Yes. Consider using replication.
		No. You do not need either replication or a GUP.

Table 38-3 Deciding whether to use more than one site with replication, a GUP, or neither *(continued)*

Question	Answer	Use multiple sites with replication or use a GUP
Do you have multiple locations with more than 1,000 clients per location?	Yes. Do you have a slow WAN link that connects to a location with more than 1,000 clients?	Yes. Consider using a GUP.
		No. You do not need either replication or a GUP.
	No Do you have a slow WAN link that connects to a location with more than 1,000 clients?	Yes. Consider using a GUP.
		No. You do not need either replication or a GUP.

When to use replication with Symantec Endpoint Protection Manager

See "Using Group Update Providers to distribute content to clients" on page 215.

See "Setting up sites and replication" on page 739.

See "Determining how many sites you need" on page 746.

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 215.
- 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 ten management servers to a database.
- Connect up to 18,000 clients (for 14.x) or 50,000 clients (for 12.1.x) 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 38-4 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.
High availability	Each site has multiple management server installations and database clustering. To handle additional clients, you add multiple management servers rather than adding multiple sites. You then use a management server list to configure client computers to automatically switch to an alternative management server if the primary management server becomes unavailable. You 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 732.

For more information on whether or not to set up replication, see the following article: When to use replication with Symantec Endpoint Protection Manager

See "What are sites and how does replication work?" on page 741.

See “Setting up sites and replication” on page 739.

See “Deciding whether or not to set up multiple sites and replication” on page 744.

How to install a second site for replication

Installing a second site for replication is a two-part process:

- Install a second Symantec Endpoint Protection Manager and database to replicate with a Symantec Endpoint Protection Manager and database that is already installed.
- Log on to the second Symantec Endpoint Protection Manager and change the schedule and the items that you want to replicate (optional).
  Changing the replication frequency and content

Installing a second site for replication

To install a second site for replication

1. Install a second Symantec Endpoint Protection Manager.

   See “Installing Symantec Endpoint Protection Manager” on page 43.

   The **Management Server Configuration Wizard** automatically starts after the management server installation.
2. In the **Management Server Configuration Wizard**, click **Custom configuration for new installation (more than 500 clients, or custom settings)**, and then click **Next**.
3. Click **Install an additional site**, and then click **Next**.
4. In the next panel, type the following information, and then click **Next**:
   - **Replication server**
     The name or IP address of the management server that is already installed and that this management server replicates with.
   - **System Administrator name** and **Password**.
     The system administrator's user name is `admin` by default. You must use a system administrator account, and not a limited administrator account or domain administrator account.
   - Check **Replicate client packages and LiveUpdate content between the local site and this partner site** (Optional).
     If you don't check this option now, you can check it later.
5. If a warning message about accepting the certificate appears, click **Yes**.
6. In the site information pane, accept or change the default values, and then click **Next**.

7 In the database choice pane, click either the **Default Embedded database** or **Microsoft SQL Server database**, and then click **Next**.

Symantec recommends that the site with which you replicate uses the same type of database, but it is not required.

Complete the installation based on the database that you choose.

8 In the **Run LiveUpdate** pane, click **Next**.

Optionally add the partner information.

9 Optionally accept the data collection feature, and then click **Next**.

The database gets created. This step takes some time.

The Symantec Endpoint Protection Manager launches.

Changing the replication frequency and content

By default, replication is scheduled to occur automatically after you install the second site and management server. Replication occurs according to the default schedule as part of installing the second management server. However, you may need to change the frequency based on how long replication takes. You can change the frequency on either the local site or the new site, but Symantec recommends that you configure replication on the new site first. The schedule on both sites is the same the next time the two sites replicate. The site with the smaller ID number initiates the scheduled replication. Whichever site is configured as the new replication partner always has its database overwritten by the database from the local site that the new site points to.

Both sites automatically share groups and policies. You can choose whether to replicate logs, client installation packages, or LiveUpdate content based on the amount of disk space that is available.

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. Both the client packages and LiveUpdate content can include a large volume of data. The data in a client package might be as large as 5 GB. The client 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.

After the initial, full database replication, subsequent replications are fairly small, if you only replicate policies, clients, and groups, and not logs. Make sure that the management servers have enough available disk space to replicate based on the frequency and content.

To change the replication frequency and schedule

1. In the console, click **Admin** > **Servers**.
2. Under **Servers** > **Local Site**, expand **Replication Partners**, and select the site you want to replicate with.
3. Under **Tasks**, click **Edit Replication Partner Properties**.
4. Choose the content you want to replicate.
5. To change the schedule, do one of the following tasks:
   - Check **Auto-replicate** to let the management server choose when to replicate the data.
     This option causes frequent and automatic replication to occur between two sites, about every 2 hours.
   - Check **Replicate on a schedule** to set up a custom schedule.
6. Click **OK**.

Replication considerations and best practices

See "Replicating data immediately" on page 750.

See "Setting up sites and replication" on page 739.

See "What are sites and how does replication work?" on page 741.

See "Deciding whether or not to set up multiple sites and replication" on page 744.

See "Disabling replication and restoring replication before and after an upgrade" on page 153.

Replicating data immediately

Replication normally occurs according to the default schedule when you set up an additional site. You might want replication to occur immediately. The site with the smaller ID number initiates the scheduled replication.

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 739.

See "How to install a second site for replication" on page 748.

To replicate data at any time

1. In the console, click **Admin** > **Servers**.
2. Under **Servers** > **Local Site**, expand **Replication Partners** and select the site.
3. Under **Tasks**, click **Replicate Now**.

4 Click **Yes**.

5 Click **OK**.

Deleting sites

Deleting a replication partner disconnects the partnership in Symantec Endpoint Protection Manager, but does not uninstall the management server software or delete the second site.

If you remove the 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.

See "Disabling replication and restoring replication before and after an upgrade" on page 153.

To delete a site

1 In the console, click **Admin** > **Servers** > **Local Site**, expand **Replication Partners**, right-click the replication partner, and click **Delete Replication Partner**.

2 Under **Remote Sites**, right-click the site and click **Delete Remote Site**.

3 Click **Yes**.

See "Setting up sites and replication" on page 739.

Chapter 39

Preparing for disaster recovery

This chapter includes the following topics:

Disaster recovery best practices

To prepare for recovery after a hardware failure or database corruption, you should back up the information that is collected after you install Symantec Endpoint Protection Manager.

Preparing for disaster recovery

Table 39-1 High-level steps to prepare for disaster recovery

Step	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 default location: `C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\data\backup` The backup file is called *date_timestamp*.zip. See "Backing up the database and logs" on page 754.
Step 2: Back up the disaster recovery file	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: `C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\Server Private Key Backup\recovery_timestamp.zip` 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 308.
Step 3: Update or back up the server certificate (optional)	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 711. See "Backing up a server certificate" on page 755.
Step 4: 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 5: Store the backup data in a secure location off-site	Copy the files you backed up in the previous steps to another computer

Performing disaster recovery

Table 39-2 lists the steps to recover your Symantec Endpoint Protection environment in the event of hardware failure or database corruption.

Before you follow these steps, make sure that you made backups and recovery files.

Table 39-2 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 756. 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 758.
Step 2: Restore the database.	You can restore the database with or without a database backup. See "Restoring the database" on page 759.
Step 3: Re-enable Federal Information Processing Standards (FIPS) 140-2 compliance. (optional)	If you use a FIPS-compliant version of Symantec Endpoint Protection and have FIPS compliance enabled, after you recover Symantec Endpoint Protection Manager, you must reenable FIPS compliance. This setting is not stored in the disaster recovery file.

See "Backing up your license files" on page 102.

See "Exporting and importing server settings" on page 717.

See: Disaster recovery best practices for Symantec Endpoint Protection 12.1.

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: `C:\Program Files (x86)\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.

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 723.

See "Disaster recovery best practices" on page 752.

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** > **Servers**.
2. Under **Servers**, click **Local Site (My Site)** > **localhost**.
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 706.

See "Generating a new server certificate" on page 758.

See "Best practices for updating server certificates and maintaining the client-server connection" on page 707.

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. Symantec Endpoint Protection Manager creates a recovery file during installation. You can also use this procedure to reconfigure the existing site, or to install an additional site for replication.

See "Disaster recovery best practices" on page 752.

To reinstall the management server

1. Uninstall the existing management server.
2. Install the server from the installation file.

   See "Installing Symantec Endpoint Protection Manager" on page 43.

3 In the **Welcome** panel, make sure that the **Use a recovery file to restore communication with previously deployed clients** option is checked, and then click **Next**.

By default, the recovery file is located in: `C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\Server Private Key Backup`. The recovery file reconnects your clients to the Symantec Endpoint Protection Manager.

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 resides on another computer or is otherwise not affected, you do not need to restore your database.

See "Restoring the database" on page 759.

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 Select one of the following options:

- To reconfigure the management server on the existing site, click **Reconfigure the management server**.
- To reconfigure the management server to replicate data with an existing site, click **Reconfigure the management server to replicate with a different site**.
  This option reconfigures the locally installed management server to create a new site and to replicate the data with another existing site in your network. Also, if you have two non-replicating sites, use this option to convert one of the sites into a site that replicates with the second site.

  Note: If you leave **Use a recovery file to restore communication with previously deployed clients** checked, the installation proceeds. However, it ignores the default domain ID in the recovery file and uses the domain ID of the replication partner. After reconfiguration completes, existing clients may fail to connect due to the change in domain ID.

3 Follow the instructions in each panel.

See "Reinstalling or reconfiguring Symantec Endpoint Protection Manager" on page 756.

Generating a new server certificate

You generate a new server certificate for Symantec Endpoint Protection Manager if the IP address or host name of the server changes, or if your private key was compromised.

By default, client-server communication depends on verifying the server certificate. If you generate a new server certificate, this verification fails and communication is interrupted. Follow the best practices for updating the certificate before you begin this procedure.

See "Best practices for updating server certificates and maintaining the client-server connection" on page 707.

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**. Make sure that **Generate new Keys** is checked, and then click **Next**.

   Generate new Keys generates a new certificate with a new key pair (public and private keys). If you uncheck this option, the new certificate uses the same key pair as before, which lowers the Symantec Endpoint Protection Manager server security profile in the case of a compromised key pair.
5. Click **Yes**, and then click **Next**.
6. You must restart the following services to use the new certificate:
   - The Symantec Endpoint Protection Manager service
   - The Symantec Endpoint Protection Manager Webserver service
   - The Symantec Endpoint Protection Manager API service

   See "Stopping and starting the management server service" on page 151.

   See "Stopping and starting the Apache Web server" on page 769.

The next time you log on to Symantec Endpoint Protection Manager, you are asked to trust the new certificate.

See "About accepting the self-signed server certificate for Symantec Endpoint Protection Manager" on page 300.

See "Logging on to the Symantec Endpoint Protection Manager console" on page 48.

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 754.

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 with a database backup

1. Stop the management server service.

   See "Stopping and starting the management server service" on page 151.
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.

Restoring the database without a database backup

You may need to restore the database without a database backup in the following cases:

- You tried and cannot reset your administrator password.
  See "Resetting a forgotten Symantec Endpoint Protection Manager password" on page 297.
- The embedded database service does not start.
- You did not make a database backup and the database is corrupted.

To restore the database without a database backup

1. Back up the policy files.

   You import the exported policy files after you reinstall the database.

   See "Exporting and importing individual Endpoint Protection policies" on page 323.

2. If you have multiple domains, create a text file named SEPBackup.txt and add any domain IDs. (Optional)

   To save the management server information, add the IP address and host name of the management server to the file.

3. Stop the management server service.

   See "Stopping and starting the management server service" on page 151.

4. Reconfigure the management server using the Management Server Configuration Wizard and the recovery file.

   See "Reinstalling or reconfiguring Symantec Endpoint Protection Manager" on page 756.

5. On the reconfigured Symantec Endpoint Protection Manager, in the following file:

   SEPM_Install`/tomcat/etc/conf.properties`

   The default for *SEPM_Install* is C:/Program files (x86)/Symantec/Symantec Endpoint Protection Manager.

   Change:

   `scm.agent.groupcreation=false` to `scm.agent.groupcreation=true`

   This edit enables the automatic creation of client groups. Otherwise, the clients to reappear in the default group as they check in.

Clients can communicate with Symantec Endpoint Protection Manager, but only re-appear in the console only after their next check-in.

Section 9

Troubleshooting Symantec Endpoint Protection Manager

Chapter 40

Troubleshooting installation and communication problems

This chapter includes the following topics:

Troubleshooting Symantec Endpoint Protection

Table 40-1 displays the most common issues that you might encounter when you install and use Symantec Endpoint Protection.

Table 40-1 Common issues you can troubleshoot

Task	Description
Fixing installation problems	You can download and run the Symantec Diagnostic Tool (SymDiag) to verify that your computers are ready for installation. The tool is provided from the Symantec Support website through Help on the management server and the client. See "Troubleshooting computer issues with the Symantec Diagnostic Tool (SymDiag)" on page 764. See "Identifying the point of failure of an installation" on page 764.
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 402. See "Removing viruses and security risks" on page 404. If a threat does attack a client computer, you can identify and respond to the threat. Virus removal and troubleshooting 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 article: Troubleshoot LiveUpdate and definition issues with Endpoint Protection Manager Symantec Endpoint Protection: LiveUpdate Troubleshooting Flowchart
Fixing communication problems	The communication channels must be open between all of the Symantec Endpoint Protection components. These channels include the following: server to client, server to database, and server and client to the content delivery component, such as LiveUpdate. See "Troubleshooting connectivity problems between Symantec Endpoint Protection Manager and the Symantec Endpoint Protection client" on page 765. See "Troubleshooting communication problems between Symantec Endpoint Protection Manager and the console or the database" on page 773. Best Practices and Troubleshooting for Group Update Providers
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 "Disaster recovery best practices" on page 752.
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 719.

Table 40-1 Common issues you can troubleshoot *(continued)*

Task	Description
Troubleshooting reporting issues	You can solve various report and log issues. See "Troubleshooting reporting issues" on page 777.
Troubleshooting replication issues	Replication Troubleshooting Flowchart for Symantec Endpoint Protection

See "What are the tools included with Symantec Endpoint Protection?" on page 837.

Troubleshooting computer issues with the Symantec Diagnostic Tool (SymDiag)

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 Diagnostic Tool (SymDiag)

1. Do one of the following tasks:
   - See: Download the Symantec Diagnostic Tool (SymDiag) to detect Symantec product issues
   - In either the Symantec Endpoint Protection Manager or the client, click **Help > Download Symantec Diagnostic 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.

See "Choosing a method to install the client using the Client Deployment Wizard" on page 119.

Troubleshooting connectivity problems between Symantec Endpoint Protection Manager and the Symantec Endpoint Protection 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 check the communication between the client and the management server in several ways.

Table 40-2 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 "Symantec Endpoint Protection client status icons" on page 165. See "Checking the connection to the management server on the client computer" on page 767. See "Investigating protection problems using the troubleshooting file on the client" on page 768.

Table 40-2 Checking the connection between the management server and the client *(continued)*

What to check	Solution
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 768. ■ Ping the management server from the client computer. See "Using the ping command to test the connectivity to the management server" on page 769. ■ 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 770.
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 711. See "Best practices for updating server certificates and maintaining the client-server connection" on page 707. 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 "Checking whether the client is connected to the management server and is protected" on page 163. ■ The client does not receive policy updates from the management server. ■ The management server shows that it does connect with the client. See "Symantec Endpoint Protection client status icons" on page 165.

Table 40-2 Checking the connection between the management server and the client *(continued)*

What to check	Solution
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.
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 771. See "Checking the inbox logs on the management server" on page 771.
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 772.

If Symantec Endpoint Protection Manager displays logging errors or HTTP error codes, see the following 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 connectivity problems between Symantec Endpoint Protection Manager and the Symantec Endpoint Protection client" on page 765.

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 connectivity problems between Symantec Endpoint Protection Manager and the Symantec Endpoint Protection client" on page 765.

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 connectivity problems between Symantec Endpoint Protection Manager and the Symantec Endpoint Protection client" on page 765.

Note: The default for *SEPM_Install* is C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager.

To enable the Apache HTTP server Access log

1. In a text editor, open the file *SEPM_Install*\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 151.

   See "Stopping and starting the Apache Web server" on page 769.

To view the Apache HTTP server Access log

1. On the management server, open the file *SEPM_Install*\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 768.

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 connectivity problems between Symantec Endpoint Protection Manager and the Symantec Endpoint Protection client" on page 765.

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 whether the problem is with the connection or network, or with the client itself.

You can also check the connection between the management server and the client computer by using the following methods:

- Checking whether the Symantec Endpoint Protection client status icon shows a green dot.
  See "Symantec Endpoint Protection client status icons" on page 165.
- Checking the connection status on the Symantec Endpoint Protection client.
  See "Checking the connection to the management server on the client computer" on page 767.

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://*SEPMServer*:8014/secars/secars.dll?hello,secars

   where *SEPMServer* is the management server's DNS name, NetBIOS name, or IP address.

   IP address includes IPv4 and IPv6. You must enclose the IPv6 address with square brackets: **http://[*SEPMServer*]:*port number***
3. When the webpage 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 connectivity problems between Symantec Endpoint Protection Manager and the Symantec Endpoint Protection client" on page 765.

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 connectivity problems between Symantec Endpoint Protection Manager and the Symantec Endpoint Protection client" on page 765.

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 connectivity problems between Symantec Endpoint Protection Manager and the Symantec Endpoint Protection client" on page 765.

See "Checking the debug log on the client computer" on page 771.

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.

   The inbox appears in the following default location on the management server computer:
   SEPM_Install\data\inbox\log

   The default for *SEPM_Install* is C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager.
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 with Communication Update Package Deployment" on page 173.

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.

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 129.

See "Troubleshooting connectivity problems between Symantec Endpoint Protection Manager and the Symantec Endpoint Protection client" on page 765.

To restore client-server communication settings by using the SylinkDrop tool for Windows

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 (Sylink.xml) manually" on page 174.

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:

- In the full product installation file from MySymantec, locate `Tools\SylinkDrop\SylinkDrop.exe`.
  See Getting Started with MySymantec.
- On the computer that runs the management server, locate `C:\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. For information on the command-line options, in the `\Tools\SylinkDrop` folder, click the readme file.

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 Symantec Endpoint Protection Manager and the console or the database

If you have a connection problem with the Symantec Endpoint Protection Manager 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 located by default in the following location:

`SEPM_Install\tomcat\logs\scm-server-0.log`

The default for *SEPM_Install* is C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager.

Table 40-3 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 774.
Check that the management server heap size is correct.	If you cannot log on to the management server's remote console, you may need to increase the Java heap size. You may also see an out-of-memory message in the scm-server log. For more information on the default heap sizes, see: Determining the default settings for the network sizes that you select during installation of the Symantec Endpoint Protection Manager
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.
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, new fixes, and system requirements for all versions of Endpoint Protection

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 40-4 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 and Host Exploit Mitigation 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.

Chapter 41

Troubleshooting reporting issues

This chapter includes the following topics:

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 article: Enabling SSL communications between a Symantec Endpoint Protection Manager and its clients

- 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 778.
- 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 following article: 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 780.

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 database connection timeout
- Change the database 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 database timeout values in Reporter.php

1. Browse to the following default folder on the Symantec Endpoint Protection Manager server:

   C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\Php\Include\Resources
2. Open the Reporter.php file with a plain-text editor, such as Notepad.

3 Find the **$CommandTimeout** and **$ConnectionTimeout** lines and increase the value (in seconds). If either 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;

$ConnectionTimeout = 600;
```

Add these new lines before the following characters: `?>`

4 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 the max_execution_time parameter in Php.ini

1 Browse to following default folder on the Symantec Endpoint Protection Manager server:

C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\Php

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 Apache timeout parameters in httpd.conf

1 Browse to the following default folder on the Symantec Endpoint Protection Manager server:

C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\apache\conf

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 standalone web browser" on page 635.

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:

IPAddress **localhost** **#***to log on to reporting functions*

where you replace *IPAddress* 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 the IPv4 for my console computer

2001:db8:85a3::8a2e:370:7334 localhost # This entry is the IPv6 address for my console computer

4 Save and close the file.

Chapter 42

Using Power Eraser to troubleshoot difficult and persistent threats

This chapter includes the following topics:

What you should know before you run Power Eraser from the Symantec Endpoint Protection Manager console

Power Eraser provides aggressive scanning and analysis to help resolve issues with heavily infected Windows computers. Because Power Eraser analysis is aggressive, it sometimes flags the critical files that you might need. Power Eraser can produce more false positives than virus and spyware scans.

Warning: You should run Power Eraser only in emergency situations, such as when computers exhibit instability or have a persistent problem. Typically, you run Power Eraser on a single computer or small group of computers. You should not run other applications at the same time. In some cases, a regular scan event alerts you to run a Power Eraser analysis.

Differences between using Power Eraser from Symantec Endpoint Protection Manager or locally with the SymDiag tool

You can run Power Eraser remotely from the management console on your Windows clients. Symantec Endpoint Protection does not include an option to launch Power Eraser directly from the client. However, a user on the client computer can download the SymDiag tool and run Power Eraser from the tool.

- If you use the SymDiag tool, Power Eraser detections do not appear in the Symantec Endpoint Protection Manager logs.
- When you run Power Eraser from the console, Power Eraser does not examine the user-specific load points, registrations, and folders that the SymDiag tool examines.

Note: Make sure that you do not run Power Eraser from the console and locally with the SymDiag tool at the same time. Otherwise, you might negatively affect the computer performance.

Power Eraser consumes a large amount of computer resources. Power Eraser files can also consume a large amount of space on the computer if you run Power Eraser on a computer multiple times. During each analysis, Power Eraser saves detection information in the files that it stores in the Symantec Endpoint Protection application folder. The files are purged when the client purges the logs.

How Power Eraser is different from virus and spyware scans

Power Eraser is different from regular scans in the following ways:

- Unlike a full scan, Power Eraser does not scan every file on the computer. Power Eraser examines load points and load point disk locations as well as running processes and installed services.
- Power Eraser detections do not appear in the Quarantine.
- Power Eraser takes precedence over virus and spyware scans. When you run Power Eraser, Symantec Endpoint Protection cancels any virus and spyware scan in progress.
- Power Eraser does not automatically remediate detections. You must review the detection list in the Scan log or Risk log and select an action from the log. You can choose to remove the detection or mark the detection as safe (leave alone). You can also restore (undo) a removed detection.

Power Eraser can run in regular mode or in rootkit mode. The rootkit mode requires a restart before the scan launches. Also, if you choose to remove any Power Eraser detection, the computer must be restarted for the remediation to complete.

Overview of the high-level steps that you perform when you need to run Power Eraser

You perform two high-level steps when you run Power Eraser from the console:

- Start a Power Eraser analysis on one computer or a small group of computers. Power Eraser does not automatically remediate any detections because of the potential for false positives.
- Use the Risk log or Scan log to review Power Eraser detections and manually request that Power Eraser remove any detections that you determine are threats. You can also acknowledge the detections that you want to ignore and leave alone.

Review the workflow for details about how to run Power Eraser from the console and how to make sure that you configure the console settings correctly.

See "Tasks to perform when you need to run Power Eraser from the Symantec Endpoint Protection Manager console" on page 784.

Overview of the Symantec Endpoint Protection Manager policy settings that affect Power Eraser

The following are the policy settings that affect Power Eraser:

- Scan settings for user interaction
  When you let users cancel any virus and spyware scan, you also let them cancel any Power Eraser analysis. However, users cannot pause or snooze Power Eraser.
  See "Allowing users to view scan progress and interact with scans on Windows computers" on page 482.
- Exceptions policy
  Power Eraser honors the following virus and spyware exceptions: file, folder, known risk, application, and trusted web domain. Power Eraser does not honor extension exceptions.
  See "Creating exceptions for Virus and Spyware scans" on page 548.
- Log retention settings
  You can take action on Power Eraser detections as long as the detections appear in the logs. The logs are purged after the period of time that is specified in the Virus and Spyware Protection policy. By default, log events are available for 14 days. You can modify the log retention setting, or after the events expire, you can run another scan and re-populate the logs.
  See "Modifying log handling and notification settings on Windows computers" on page 478.
- Restart options

You can configure the restart settings specifically for rootkit analysis when you choose to run Power Eraser in rootkit detection mode. The administrator must have restart privileges. After you choose to remove a Power Eraser detection, the computer uses the group restart settings. Power Eraser does not use the rootkit restart settings to restart and complete a remediation.

See "Restarting the client computers from Symantec Endpoint Protection Manager" on page 127.

- Reputation queries

  Power Eraser uses the Symantec Insight server in the cloud when it scans and makes decisions about files. If you disable reputation queries, or if the client computer cannot connect to the Insight server, Power Eraser cannot use Symantec Insight. Without Symantec Insight, Power Eraser makes fewer detections, and the detections it makes are more likely to be false positives. Reputation queries are enabled when the **Allow Insight lookups for threat detection** option is enabled. The option is enabled by default.

  See "How Symantec Endpoint Protection uses Symantec Insight to make decisions about files" on page 446.

- Submissions

  Symantec Endpoint Protection sends the information about Power Eraser detections to Symantec when the **Antivirus detections** option is enabled. The option is enabled by default.

  See "Understanding server data collection and client submissions and their importance to the security of your network" on page 486.

See "Troubleshooting computer issues with the Symantec Diagnostic Tool (SymDiag)" on page 764.

Tasks to perform when you need to run Power Eraser from the Symantec Endpoint Protection Manager console

Typically you need to run a Power Eraser analysis when the Risk log shows a failed repair and recommends that you run Power Eraser. You also might run Power Eraser when a computer becomes unstable and appears to have malware or a virus that cannot be removed.

Warning: Use Power Eraser carefully. The analysis is aggressive and prone to false positives.

See "What you should know before you run Power Eraser from the Symantec Endpoint Protection Manager console" on page 781.

You can run Power Eraser from Symantec Endpoint Protection Manager on Windows client computers only.

Note: Power Eraser runs in one of two modes: without rootkit detection or with rootkit detection. The rootkit detection analysis requires a restart. The administrator must have restart privileges to run Power Eraser with rootkit detection.

Table 42-1 Tasks to perform when you need to run Power Eraser from the Symantec Endpoint Protection Manager console

Task	Description
Set administrator privileges to run Power Eraser	To run Power Eraser on client computers, administrators must have the following command access rights: ■ **Start Power Eraser Analysis** ■ **Restart Client Computers** (required to run Power Eraser with rootkit detection) See "Adding an administrator account and setting access rights" on page 282.
Set the log retention policy	The log retention setting affects how long the events are available for you to perform the Power Eraser remediate and restore actions. You can modify the log retention setting if you want more time to consider these actions. Alternately, you can run Power Eraser again to re-populate the logs. The log retention setting is part of the miscellaneous options in the Virus and Spyware Protection policy. See "Modifying log handling and notification settings on Windows computers" on page 478.
Make sure that your clients have Internet connectivity	Your client computers require Internet access so that Power Eraser can use Symantec Insight reputation data to make decisions about potential threats. Intermittent or non-existent Internet access means that Power Eraser cannot use Symantec Insight. Without Symantec Insight, Power Eraser makes fewer detections, and the detections it produces are more likely to be false positives.

Table 42-1 Tasks to perform when you need to run Power Eraser from the Symantec Endpoint Protection Manager console *(continued)*

Task	Description
Start a Power Eraser analysis on a client computer from Symantec Endpoint Protection Manager	Choose whether to run Power Eraser in regular mode or rootkit mode. You can issue the Power Eraser command from several places in Symantec Endpoint Protection Manager: ■ **Clients** page ■ Computer Status log ■ Risk log **Note:** A user on the client computer cannot run Power Eraser directly from the client user interface. Power Eraser is available as part of the SymDiag tool. However, if a client user runs the tool, the resulting logs that include Power Eraser detections are not sent to Symantec Endpoint Protection Manager. See "Starting Power Eraser analysis from Symantec Endpoint Protection Manager" on page 788. You can view the status of the command in the Computer Status log. You can filter the log so that only Power Eraser commands appear for ease of viewing. After you run Power Eraser, you view the results in the Scan log or the Risk log. The Scan log shows whether or not scan results are pending.
Cancel a Power Eraser command or action on a client computer	To cancel the Power Eraser command, use the Command Status log. **Note:** You cannot cancel Power Eraser running in rootkit mode after the restart prompt appears on the client computer. After the restart, only the computer user can cancel Power Eraser if the Virus and Spyware Protection policy lets users cancel scans. If you cancel the Power Eraser command, you also cancel any pending actions that are associated with any Power Eraser analysis, including any remediation or undo actions. See "Running commands on client computers from the console" on page 253.

Table 42-1 Tasks to perform when you need to run Power Eraser from the Symantec Endpoint Protection Manager console *(continued)*

Task	Description
View Power Eraser detections from the logs	You can view Power Eraser detections from the following logs in Symantec Endpoint Protection Manager: ■ Scan log The Scan log has a **Scan type** filter to display only Power Eraser results. The view also indicates whether or not scan results are pending. You can select **Detections** in the filtered view to display the **Power Eraser Detections** view. ■ Risk log The Risk log provides a similar filter for Power Eraser detections. However, the Risk log does not show whether or not scan results are pending. ■ Computer Status log The Computer Status log might include report icons in the **Infected** column. The event details icon links to a report that shows all current threats that cannot be remediated. The report includes log-only detections and unresolved detections. The report might recommend that you run Power Eraser on some computers. A Power Eraser icon links to a report that shows any Power Eraser detections on the computer that require administrator action. These icons also appear in the **Health State** column on the **Clients** page. See "Viewing logs" on page 655.
Check for the notifications that recommend that you run Power Eraser on client computers	By default, the administrator receives a notification when a regular scan cannot repair an infection and Power Eraser is recommended. You can check for the **Power Eraser recommended** notification on the **Monitors > Notifications** page. See "Viewing and acknowledging notifications" on page 669.
View Power Eraser detections on the **Command Status** page	You can access reports about Power Eraser detections on the **Command Status** page. An event details icon appears in the **Completion Status** column. The icon links to a report that shows information about detections that were made by the **Start Power Eraser Analysis** command and any other scan command. The command status details option gives you information about a particular scan. You can click on the event details icon to get information about a particular client computer. See "Running commands on client computers from the console" on page 253.

Table 42-1 Tasks to perform when you need to run Power Eraser from the Symantec Endpoint Protection Manager console *(continued)*

Task	Description
View Power Eraser detections from the Clients tab	You can access reports about Power Eraser detections from the **Clients** tab on the **Clients** page. Report icons appear in the **Health State** column if information is available. The event details icon links to a report that shows all current threats that cannot be remediated. The report includes any Power Eraser detections. A Power Eraser icon links to a report that shows any Power Eraser detections on the computer that require administrator action. The icons also appear in the Computer Status log. See "Viewing the protection status of client computers" on page 247.
Remediate or restore Power Eraser detections from the Scan log or Risk log in Symantec Endpoint Protection Manager	Unlike other Symantec Endpoint Protection scans, Power Eraser does not automatically remediate detected threats. Power Eraser analysis is aggressive and might detect many false positives. After you determine that the detection requires remediation, you must initiate a remediation manually. You can also undo (restore) a Power Eraser detection that you remediated. See "Responding to Power Eraser detections" on page 790.

Starting Power Eraser analysis from Symantec Endpoint Protection Manager

You can run Power Eraser to analyze and detect persistent threats on a single computer or a small group of computers.

See "What you should know before you run Power Eraser from the Symantec Endpoint Protection Manager console" on page 781.

After Power Eraser detects potential risks, you view the risks and determine which risks are threats. Power Eraser does not automatically remediate risks. You must manually run Power Eraser to remediate the risks that you determine are threats. You can also run Power Eraser on a particular threat or threats that other protection features detect. Power Eraser runs on the computers that are associated with the detection.

See "Tasks to perform when you need to run Power Eraser from the Symantec Endpoint Protection Manager console" on page 784.

See "Responding to Power Eraser detections" on page 790.

Note: When you run Power Eraser in rootkit mode, and the restart option message appears on the client computer, the administrator or the user cannot cancel Power Eraser. After the restart, the user can cancel Power Eraser if the Virus and Spyware Protection policy lets users cancel scans.

To start Power Eraser analysis from the Clients page in Symantec Endpoint Protection Manager

1. On the **Clients** page, on the **Clients** tab, select the computers that you want to analyze.

   If you select many computers, you might adversely affect the performance of your network.
2. Under **Tasks**, click **Run command on computers**, and then click **Start Power Eraser Analysis**.
3. In the **Choose Power Eraser** dialog, select whether or not you want Power Eraser to run in rootkit mode. For rootkit mode, you can set the restart options. You must have administrator privileges to set restart options and run a rootkit scan.
4. Click **OK**.

   Power Eraser runs on the select computers. You can cancel the command on the **Command Status** tab on the **Monitors** page.

To start Power Eraser analysis from the Computer Status log in Symantec Endpoint Protection Manager

1. In the console, in the sidebar, click **Monitors** and select the **Logs** tab.
2. In the **Log type** list box, select the **Computer Status** log, and then click **View Log**.
3. Select the computers on which you want to run Power Eraser and select **Start Power Eraser Analysis** from the **Commands** drop-down box.

   If you select many computers, you might adversely affect the performance of your network.
4. Click **Start**.
5. In the **Choose Power Eraser** dialog, select whether or not you want Power Eraser to run in rootkit mode. For rootkit mode, you can set the restart options. You must have administrator privileges to set restart options and run a rootkit scan.
6. Click **OK**.

   Power Eraser runs on the selected computers. You can cancel the command on the **Command Status** tab.

To start Power Eraser analysis from the Risk log in Symantec Endpoint Protection Manager

1. In the console, in the sidebar, click **Monitors** and select the **Logs** tab.
2. In the **Log type** list box, select the **Risk** log, and then click **View Log**

3 Select the risks on which you want to run Power Eraser. In the **Event Action** column, you might see an alert to run Power Eraser.

You can run Power Eraser on any risk in the log.

4 Select **Start Power Eraser Analysis** from the **Action** drop-down or the **Action** column.

5 Click **Start**.

6 In the **Choose Power Eraser** dialog, select whether or not you want Power Eraser to run in rootkit mode. For rootkit mode, you can set the restart options. You must have administrator privileges to set restart options and run a rootkit scan.

7 Click **OK**.

Power Eraser runs on the computers that are infected with the selected risks. You can cancel the command on the **Command Status** tab.

Responding to Power Eraser detections

Power Eraser does not remediate any detections during a scan because its aggressive detection capability is prone to false positives. You must request remediation for detected events from the logs after you review the detections and decide whether to remediate them or leave them alone. If you choose remediation, Power Eraser removes the files that are associated with the detection. However, you can restore the removed files until the logs are purged.

The log retention policy determines how long Power Eraser events are available. By default, the events are available for 14 days.

See "Tasks to perform when you need to run Power Eraser from the Symantec Endpoint Protection Manager console" on page 784.

See "What you should know before you run Power Eraser from the Symantec Endpoint Protection Manager console" on page 781.

To respond to Power Eraser detections

1 Make sure that the Power Eraser analysis completed.

- The Computer Status log includes an icon that indicates the scan is complete.
- The Scan log shows whether or not Power Eraser finished the analysis.

2 In the Risk log or on the **Scan log > View detections** page, select a single detection or multiple detections to which to apply an action.

- Next to a particular risk that is labeled **Potential risk found (Pending admin action)**, click the plus icon in the **Action** column.
- Select multiple risks that are labeled **Potential risk found (Pending admin action)**, and then select the action from the **Action** drop-down menu.

3 Choose one of the following actions:

- **Delete risk that Power Eraser detected**
  Remediates the risk by removing it from the computer. Power Eraser saves a safe backup file that can be restored.
- **Ignore risk that Power Eraser detected**
  Acknowledges that you reviewed the detection and do not want to remediate the risk.

  Note: This action changes the event action to "Left alone by Admin" in the management console logs only. The acknowledgement does not update the corresponding event action on the client. The client log view continues to show the event action as "Pending analysis."

4 If you selected an action from the **Action** drop-down menu, click **Apply**.

If you selected **Ignore risk that Power Eraser detected**, the detection now appears as **Potential risk found (left alone)**.

You can restore a removed detection that is labeled **Potential risk found (Removed)** by selecting the **Restore risk that Power Eraser deleted** action.

Table 42-2 Summary of Power Eraser detection states

Detection state	Description
Pending admin action	Power Eraser detected the risk as a potential threat. You should review the risk and decide if Power Eraser should remediate the risk or acknowledge the risk and leave it alone.
Restored	An administrator restored any files that were moved when an administrator requested that Power Eraser remediate the risk.
Deleted	An administrator requested that Power Eraser remediate and delete the risk. When Power Eraser deletes a risk, it deletes the files that are associated with the risk but makes safe backup copies that can be restored. You might want to restore a deleted risk that you later determine is not a risk. You can restore the files until the log events are purged.
Left alone by admin	An administrator requested that Power Eraser leave the risk alone.

Appendix A

Client feature comparison tables

This appendix includes the following topics:

Symantec Endpoint Protection feature dependencies for Windows clients (12.1.x through 14.x)

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 A-1 Dependencies of protection features

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.

Table A-1 Dependencies of protection features *(continued)*

Feature	Interoperability Notes
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. If you disable Download Insight, you disable portal detections. This means that Auto-Protect and scheduled and on-demand scans evaluate all files as non-portal files and use a sensitivity level that is determined by Symantec. See "Managing Download Insight detections" on page 442.

Table A-1 Dependencies of protection features *(continued)*

Feature	Interoperability Notes
Insight Lookup (12.1.x clients) and cloud protection	Insight Lookup uses the Symantec Insight reputation database in the cloud to make decisions about files that were downloaded from a supported portal. Starting in 14: ■ The Insight Lookup functionality runs automatically as part of Auto-Protect, scheduled scans, and on-demand scans on standard and embedded/VDI clients. The standard and embedded/VDI clients support cloud-enabled content. ■ You can enable or disable Insight Lookup in the scan settings for any 12.1.x clients you have, but you can no longer configure a specific sensitivity level for Insight Lookup. Legacy Insight Lookup now uses the sensitivity level that is set in the Download Insight policy. See "How Windows clients receive definitions from the cloud" on page 412. Cloud scans and 12.1.x Insight Lookup have the following feature dependencies: ■ Insight lookups must be enabled. Otherwise, cloud scans and Insight Lookup cannot function. ■ Download Insight must be enabled so that files can be marked as portal files. ■ If Download Insight is disabled, cloud scans and Insight Lookup continue to function. They use a sensitivity level that is automatically set by Symantec that detects only the most malicious files. **Note:** (12.1.x clients only) Cloud lookups do not apply to right-click scans of folders or drives on your client computers. However, cloud lookups do apply to right-click scans of selected portal files.
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. See "Managing SONAR" on page 495.

Table A-1 Dependencies of protection features *(continued)*

Feature	Interoperability Notes
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.
Custom IPS signatures	Uses the firewall. See "Managing custom intrusion prevention signatures" on page 387.
Power Eraser	Uses Insight lookups. Power Eraser uses reputation information to examine files. Power Eraser has a default reputation sensitivity setting that you cannot modify. If you disable the option **Allow Insight lookups for threat detection**, Power Eraser cannot use reputation information from Symantec Insight. Without Insight, Power Eraser makes fewer detections, and the detections are more likely to be false positives. **Note:** Power Eraser uses its own reputation thresholds that are not configurable in Symantec Endpoint Protection Manager. Power Eraser does not use the Download Insight settings. See "What you should know before you run Power Eraser from the Symantec Endpoint Protection Manager console" on page 781.
Memory Exploit Mitigation	Intrusion prevention must be installed. Intrusion prevention can be enabled or disabled.

See "Choosing which security features to install on the client" on page 121.

Symantec Endpoint Protection features based on platform (12.1.x through 14.x)

- Exceptions policy settings based on platform
- **Device Control** differences based on platform

See "How to choose a client installation type" on page 118.

See "Symantec Endpoint Protection feature dependencies for Windows clients (12.1.x through 14.x)" on page 792.

Client protection features based on platform

Table A-2 lists which protection features are available on Windows clients, Mac clients, and Linux clients.

Table A-2 Client protection features based on platform

Client feature	Windows	Mac	Linux
Virus and Spyware Protection	Yes	Yes	Yes
Network and Host Exploit Mitigation ■ Network Threat Protection (intrusion prevention and firewall) ■ Memory Exploit Mitigation (introduced as Generic Exploit Mitigation in 14)	Yes	■ Firewall (as of 14.2) ■ Intrusion prevention (as of 12.1.4) Intrusion prevention for the Mac does not support custom signatures.	No
Proactive Threat Protection ■ Application and Device Control ■ SONAR	Yes	Device Control only (as of 14)	No
Host Integrity	Yes	No	No
Other protections ■ System lockdown ■ Tamper Protection	Yes	No	No

See "About application control, system lockdown, and device control" on page 502.

See "How Host Integrity works" on page 605.

Management features based on platform

Table A-3 lists the management features that are available on Windows clients, Mac clients, and Linux clients.

Table A-3 Management features based on platform

Management feature	Windows	Mac	Linux
Deploy clients remotely from Symantec Endpoint Protection Manager ■ Web link and email ■ Remote push ■ Save package	Yes	Yes	Yes (**Web link and email**, **Save package** only)
Run commands on clients from the management server	■ Scan ■ Update content ■ Update content and scan ■ Start Power Eraser analysis (as of 12.1.5) ■ Restart client computers ■ Enable Auto-Protect ■ Enable Network Threat Protection ■ Disable Network Threat Protection ■ Enable Download Insight ■ Disable Download Insight ■ Collect File Fingerprint List (as of 12.1.6) ■ Delete from Quarantine** ■ Cancel all scans**	■ Scan ■ Update content ■ Update content and scan ■ Restart client computers (hard restart only) ■ Enable Auto-Protect ■ Enable Network Threat Protection (as of 12.1.4) ■ Disable Network Threat Protection (as of 12.1.4)	■ Scan ■ Update content ■ Update content and scan ■ Enable Auto-Protect
Enable learned applications and Network Application Monitoring	Yes	No	No
Create locations and set security policies that apply by location	Yes	Yes	No You can view the client's location by the command line, but the client does not automatically switch locations based on specific criteria.

Table A-3 Management features based on platform *(continued)*

Management feature	Windows	Mac	Linux
Set restart options for clients	Yes	No	No
Quick reports and Scheduled reports	■ Audit ■ Application and Device Control ■ Compliance ■ Computer status ■ Deception (14.0.1) ■ Network and Host Exploit Mitigation ■ Risk ■ Scan ■ System	■ Computer status ■ Network and Host Exploit Mitigation ■ Risk ■ Scan	■ Audit ■ Computer status ■ Risk ■ Scan ■ System
Set size and retention options for logs that are maintained on the client computers	■ System ■ Security and risk ■ Security ■ Traffic ■ Packet ■ Control	■ System ■ Security and risk ■ Security	■ System ■ Security and risk
Password protecting the client	Yes	Uninstall the client (14.0.1)	No
Move clients to a different management server by running the SylinkDrop tool	Yes	Yes	No
Move clients to a different management server by redeploying a client package with the **Communication update package deployment** option	Yes	Yes	No

Table A-3 Management features based on platform *(continued)*

Management feature	Windows	Mac	Linux
Configure client submissions of pseudonymous security information to Symantec	Yes	(12.1.4 and later) The Submissions setting only controls antivirus detection information. You can manually disable or enable intrusion prevention submissions on the clients. How to disable IPS data submission on Symantec Endpoint Protection for Mac clients	No
Configure clients to securely submit pseudonymous system and usage information	Yes	No	No
Manage the external communication between the management server and the clients	Yes	For LiveUpdate only	No
Manage client communication settings	■ Management server lists ■ Communication mode (push or pull) ■ Set heartbeat interval ■ Upload learned applications ■ Upload critical events immediately ■ Set download randomization ■ Set reconnection preferences	■ Management server lists ■ Communication mode (push or pull) ■ Set heartbeat interval ■ Set download randomization ■ Set reconnection preferences	■ Management server lists ■ Communication mode (push or pull) ■ Set heartbeat interval

Table A-3 Management features based on platform *(continued)*

Management feature	Windows	Mac	Linux
Configure clients to use private servers (12.1.6) ■ Endpoint Detection and Response server for Insight lookups and submissions ■ Private Insight server for Insight lookups	Yes	No	No
Automatically upgrade the Symantec Endpoint Protection client with AutoUpgrade	Yes	Yes (14)	No
Automatically uninstall existing third-party security software	Yes	No	No
Automatically uninstall a problem Symantec Endpoint Protection client	Yes (14)	No	No
Authentication for Symantec Endpoint Protection Manager log on	■ Symantec Endpoint Protection Manager authentication ■ Two-factor authentication (14.2) ■ RSA SecurID authentication ■ Directory authentication ■ Smart card (PIV/CAC) authentication (14.2)	Not applicable	Not applicable

**You can only run these commands when viewing logs in Symantec Endpoint Protection Manager.

See "What are the commands that you can run on client computers?" on page 250.

See "Tasks to perform when you need to run Power Eraser from the Symantec Endpoint Protection Manager console" on page 784.

See "Monitoring the applications and services that run on client computers" on page 331.

See "Managing the client-server connection" on page 161.

See "Restoring client-server communications with Communication Update Package Deployment" on page 173.

AutoUpgrade differences based on platform

Table A-4 lists the differences in the AutoUpgrade feature between Windows clients and Mac clients.

Table A-4 AutoUpgrade differences based on platform

Feature	Windows	Mac
Delta package	Standard and dark network clients receive a delta upgrade package that Symantec Endpoint Protection Manager generates. Embedded clients receive the full install package for an upgrade.	Mac clients always receive a full install package for upgrade.
Configuration options	Include a custom installation folder, and the option to uninstall existing security software.	Only for restart and upgrade. You cannot customize the installation folder. Installation logging always writes to `/tmp/sepinstall.log`.
Restart options after the upgrade completes in **Client Install Settings**	Include an option to not to restart the Windows client computer.	Do not include an option to not restart. Mac client computers always restart after the upgrade completes.
Upgrade Clients with Package wizard	You can modify the feature set on the Windows client.	You cannot modify the feature set on the Mac client.
Upgrades from an earlier version	You can upgrade to the latest version of Symantec Endpoint Protection from any earlier version, based on the supported upgrade path.	Not supported for an upgrade from version 12.1.6.x or earlier. For example, you cannot upgrade from 12.1.6.4 to 14 using AutoUpgrade.

See "Upgrading client software with AutoUpgrade" on page 156.

See "Supported upgrade paths to the latest version of Symantec Endpoint Protection 14.x" on page 144.

See "How to choose a client installation type" on page 118.

Virus and Spyware Protection policy settings based on platform

Table A-5 lists the differences in the settings that are available for Windows clients, Mac clients, and Linux clients.

Table A-5 Virus and Spyware Protection policy settings based on platform

Policy setting	Windows	Mac	Linux
Administrator-defined scans	■ Scheduled scans (Active, Full, Custom) ■ On-demand scans ■ Triggered scans ■ Startup scans ■ Retry missed scheduled scans ■ Randomized scheduled scans	■ Scheduled scans (Custom) ■ On-demand scans ■ Retry missed scheduled scans	■ Scheduled scans (Custom) ■ On-demand scans ■ Retry missed scheduled scans
Auto-Protect	■ Enable Auto-Protect ■ Scan all files ■ Scan only selected extensions ■ Determine file types by examining file contents ■ Scan for security risks ■ Scan files on remote computers (14) ■ Scan when files are accessed, modified, or backed up ■ Scan floppies for boot viruses, with the option to delete the boot virus or log it only ■ Always delete newly created infected files or security risks ■ Preserve file times ■ Tune scan performance for scan speed or application speed ■ Emulator for packed malware (14)	■ Enable Auto-Protect ■ Automatically repair infected files ■ Quarantine files that cannot be repaired ■ Scan compressed files ■ Scan all files ■ Scan only selected folders ■ Scan everywhere except in selected folders ■ Scan for security risks Scan on mount, current clients: ■ Data disks ■ All other disks and devices Scan on mount, legacy clients (12.1.3 and earlier): ■ Music or video disks ■ iPod players ■ Show progress during scan	■ Enable Auto-Protect ■ Scan all files ■ Scan only selected extensions ■ Scan removable media ■ Scan for security risks ■ Scan files on remote computers ■ Scan when files are accessed or modified ■ Scan inside compressed files

Table A-5 Virus and Spyware Protection policy settings based on platform *(continued)*

Policy setting	Windows	Mac	Linux
Email scans	■ Microsoft Outlook Auto-Protect ■ Internet email Auto-Protect (removed in 14.2 RU1) ■ Lotus Notes Auto-Protect (removed in 14.2 RU1)	No	No
What to scan	■ Additional locations ■ Memory ■ Selected folders ■ Selected extensions ■ Storage migration locations ■ Files inside compressed files ■ Security risks	■ All or selected folders ■ Hard drives and removable drives ■ Files inside compressed files	■ All files ■ All or selected folders ■ Selected extensions ■ Files inside compressed files ■ Security risks
User-defined scans (client)	■ Active scan ■ Full scan ■ Custom scan of individual folders, files, and extensions	■ Full scan ■ Custom scan of individual folders and files	■ Full scan ■ Custom scan of individual folders and files
Define remediation actions for detections	■ Clean (only applies to malware) ■ Quarantine ■ Delete ■ Leave alone (log only) The actions apply to categories of malware and security risks that Symantec periodically updates.	■ Repair infected files ■ Quarantine files that cannot be repaired	■ Clean (only applies to malware) ■ Quarantine ■ Delete ■ Leave alone (log only)

Table A-5 Virus and Spyware Protection policy settings based on platform *(continued)*

Policy setting	Windows	Mac	Linux
Set actions to take while a scan is running	■ Stop the scan ■ Pause a scan ■ Snooze a scan ■ Scan only when the computer is idle	(12.1.4) ■ Stop a scan ■ Pause a scan ■ Snooze a scan before it begins ■ Snooze a scan that is in progress (through 12.1.6x only) ■ Scan only when the computer is idle	No
Download Insight	Yes	No	No
Insight lookups for threat detection	Yes	No	No
Bloodhound	Yes	No	No
SONAR	Yes Scans of remote computers (14) Suspicious Behavior Detection (14)	No	No
Early Launch Anti-Malware Driver	Windows 8 and later, and Windows Server 2012 and later	No	No
Power Eraser	Yes (12.1.5)	No	No
Endpoint Detection and Response enablement	Yes (12.1.6)	No	No
Shared Insight Cache	Yes vShield-enabled (12.1.6 and earlier)	No	No
Virtual Image Exception	Yes	No	No

See "Preventing and handling virus and spyware attacks on client computers" on page 402.

See "Using Symantec Endpoint Protection in virtual infrastructures" on page 675.

Firewall, Intrusion Prevention, and Memory Exploit Mitigation, settings based on platform

Table A-6 displays the differences in the settings that are available for Windows clients and Mac clients

Table A-6 Intrusion Prevention policy settings based on platform

Policy setting	Windows	Mac (12.1.4)
Exceptions for intrusion prevention signatures	Yes **Note:** Custom exceptions are not supported for Browser Protection signatures.	Yes
Show or hide user notifications	Yes	Yes
Enable or disable excluded hosts	Yes	Yes
Custom IPS signatures	Yes	No
Enable or disable Network Intrusion Prevention	Yes	Yes
LiveUpdate updates IPS content	Yes	Yes
The management server updates IPS content	Yes	No **
Client package includes IPS	Yes	Yes
Network intrusion prevention	Yes	Yes
Browser intrusion prevention	Yes ■ Log-only mode (12.1.6)	No
Excluded hosts (network intrusion prevention)	Yes	Yes

**You can set up the Apache web server that installs with Symantec Endpoint Protection Manager as a reverse proxy for LiveUpdate content. See:

Enabling Mac and Linux clients to download LiveUpdate content using the Apache Web server as a reverse proxy

See "Managing intrusion prevention" on page 377.

Table A-7 Memory Exploit Mitigation policy settings based on platform

Policy setting	Windows	Mac (12.1.4)
Memory Exploit Mitigation Generic Exploit Mitigation (14 MPx)	Yes (14) ■ Fine-tuning false positives (14.0.1) ■ Custom applications (14.1, cloud only)	No

See "Hardening Windows clients against memory tampering attacks with a Memory Exploit Mitigation policy" on page 393.

LiveUpdate policy settings based on platform

Table A-8 displays the differences in the LiveUpdate settings that are available for Windows clients, Mac clients, and Linux clients.

Table A-8 LiveUpdate policy settings based on platform

Policy setting	Windows	Mac	Linux
Use the default management server	Yes	No **	No **
Use a LiveUpdate server (internal or external)	Yes	Yes	Yes
Use a Group Update Provider	Yes	No	No
Enable third-party content management	Yes	No	No
Enable/disable definitions	Yes	Yes	No
Reduced-size definitions (12.1.6)	Yes	No	No
Run Intelligent Updater to update content	■ Virus and spyware definitions ■ SONAR (12.1.3 and later) ■ IPS definitions (12.1.3 and later)	Virus and spyware definitions	Virus and spyware definitions

Table A-8 LiveUpdate policy settings based on platform *(continued)*

Policy setting	Windows	Mac	Linux
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**.	Yes
LiveUpdate schedule settings	■ Frequency ■ Retry window ■ Download randomization ■ Run when computer is idle ■ Options for skipping LiveUpdate	■ Frequency ■ Download randomization	■ Frequency ■ Retry window ■ Download randomization
Use standard HTTP headers (12.1.6 and earlier)	Yes, by default	Yes, by default	Yes, by default
Client security patches	Yes (14)	No	No
Application control content	Yes (14.2)	No	No

** You can set up the Apache web server that installs with Symantec Endpoint Protection Manager as a reverse proxy for LiveUpdate content. See:

Enabling Mac and Linux clients to download LiveUpdate content using the Apache Web server as a reverse proxy

See "How to choose a client installation type" on page 118.

See "How to update content and definitions on the clients" on page 178.

See "Using Intelligent Updater files to update content on Symantec Endpoint Protection clients" on page 223.

Integrations policy settings based on platform

Table A-10 displays the Integrations policy settings.

Table A-9 Integrations policy settings based on platform

Policy setting	Windows	Mac	Linux
Web Security Services (WSS) Traffic Redirection (WTR)	Yes	Yes (14.2)	No

Table A-9 Integrations policy settings based on platform *(continued)*

Policy setting	Windows	Mac	Linux
Local Proxy Service (part of WTR as of 14.2)	Yes	No Macs ignore the setting.	No

See "Configuring WSS Traffic Redirection" on page 564.

Exceptions policy settings based on platform

Table A-10 displays the Exceptions policy settings.

Table A-10 Exceptions policy settings based on platform

Policy setting	Windows	Mac	Linux
Server-based exceptions	■ Applications ■ Applications to monitor ■ Extensions ■ Files ■ Folders ■ Known risks ■ Trusted web domains ■ Tamper Protection exceptions ■ DNS or Host file change exceptions ■ Certificate (14.0.1)	■ Security risk exceptions for files or folders	■ Folders ■ Extensions
Client restrictions (Controls which restrictions end users can add on the client computer)	Yes	No	No

See "Managing exceptions in Symantec Endpoint Protection" on page 544.

Device Control differences based on platform

Table A-11 lists the differences in the **Device Control** feature between Mac and Windows.

Application control runs on Windows computers only.

Table A-11 Device Control differences based on platform

Windows	Mac
Device control works based only on Class ID (GUID) and Device ID.	Device control works at the file system level. Volume-level tasks (such as those that can be performed via command line or Disk Utility) are unaffected.
Device control performs wildcard matches on Class ID or Device ID with the star character or asterisk (`*`).	Device control performs regular expression (regexp) matches, and are limited to the following specific operations: ■ `.` (dot) ■ `\` (backslash) ■ `[set]`, `[^Set]` (set) ■ `*` (star character or asterisk) ■ `+` (plus)
The Hardware Device list includes many common device types by default.	You can choose from only five device types: ■ Thunderbolt ■ CD/DVD ■ USB ■ FireWire ■ Secure Digital (SD) Card You do not use the Hardware Device list.
You can add additional custom devices to the Hardware Device list by Class ID or Device ID.	You cannot add additional custom devices.
Devices to block (or to exclude from blocking) are derived only from the Hardware Device list. The list includes those default common device types, as well as custom devices you may have added.	Devices to block (or exclude from blocking) are selected from the device types noted above. The vendor, model, and serial number can be left blank, or can be defined by regular expression (regexp) queries. You can use regular expressions to define a range of similar devices, such as from different vendors, model, serial number ranges, and so on.
You can add more than one device type at a time.	You can only add one device type at a time.
The actions to take are to block, or to exclude from blocking (allow).	The actions to take are to block, or to exclude from blocking (allow) with mount permissions. The following mount permissions are supported: ■ Read only ■ Read and write ■ Read and execute ■ Read, write, and execute

Table A-11 Device Control differences based on platform *(continued)*

Windows	Mac
You can customize the client notification for device control.	You cannot customize the client notifications for device control.

See "Managing device control" on page 538.

Appendix B

Customizing and deploying the Windows client installation by using third-party tools

This appendix includes the following topics:

Installing Windows 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.

You can also deploy Symantec Endpoint Protection in an environment that you manage with a **Symantec Software Management Solution powered by Altiris**. You can deploy Symantec Endpoint Protection from one of the Software Management Solution suites with one of the following policies:

- A **Managed Software Delivery** policy
- A **Quick Delivery** policy

For more information, refer to the Software Management Solution suite product Help, or see:

Symantec Software Management Solution product landing page

Table B-1 Third-party tools to install the client

Tool	Description
Windows Installer 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 813. See "About configuring MSI command strings" on page 813. See "About configuring Setaid.ini" on page 814. See "Symantec Endpoint Protection command-line client features" on page 816. See "Symantec Endpoint Protection command-line client installation properties" on page 815. See "Windows Installer parameters" on page 817. See "Command-line examples for installing the Windows client" on page 821. See "Windows Security Center properties" on page 819.

Table B-1 Third-party tools to install the client *(continued)*

Tool	Description
Microsoft SMS 2003	You can install the client by using Microsoft Systems Management Server. See "Installing Windows clients with Microsoft SCCM/SMS" on page 821.
Windows Active Directory	You can use a Windows Active Directory Group Policy Object if the client computers and are members of a Windows Active Directory domain. The client computers must also use a supported Windows operating system. See "Installing Windows clients with an Active Directory Group Policy Object (GPO)" on page 822. See "Uninstalling client software with an Active Directory Group Policy Object" on page 827.
Virtualization software	You can install the client in virtual environments. See "Supported virtual installations and virtualization products" on page 81.

See "Exporting client installation packages" on page 136.

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 the installation of Symantec Endpoint Protection Manager.

Installation features and properties are specified in the following 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 Setaid.ini for a customized 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 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 814.

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.

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

See "Symantec Endpoint Protection command-line client features" on page 816.

See "Symantec Endpoint Protection command-line client installation properties" on page 815.

See "Windows Installer parameters" on page 817.

Symantec Endpoint Protection command-line 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.

Table B-2 Symantec Endpoint Protection client installation properties *(continued)*

Property	Description
CACHE_INSTALLER=*val*	Determines whether the installation files cache on the client, where *val* is one of the following values: ■ 1: Caches the installation files (default). ■ 0: Does not cache the installation files.
MIGRATESETTINGS=*val*	Determines the status of preserved settings in an upgrade scenario, where *val* is one of the following values: ■ 0: Does not preserve the settings or logs. ■ 1: Preserves all settings and logs. ■ 2: Preserves Sylink.xml and logs only.
ADDSTARTMENUICON=*val*	Determines whether or not to add the program to the Start Menu folder, where *val* is one of the following values: ■ 0: Does not add the program to the Start Menu folder. ■ 1: Adds the program to the Start Menu folder (default).

Symantec Endpoint Protection command-line client features

You can install the protection features 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 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 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

Table B-3 Symantec Endpoint Protection client features *(continued)*

Feature	Description	Required parent features
NotesSnapin	Installs the Lotus Notes Auto-Protect email feature. Applies only to versions earlier than 14.2 RU1.	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. Applies only to versions earlier than 14.2 RU1.	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 and Host Exploit Mitigation 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 installation file for the Symantec Endpoint Protection client. If the file name 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 file. If the file name contains spaces, enclose the file name in quotations. If the 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, 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
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 for 32-bit computers is C:\Program Files\Symantec\Symantec Endpoint Protection. The default directory for 64-bit computers is C:\Program Files (x86)\Symantec\Symantec Endpoint Protection. Optional

Table B-4 Windows Installer parameters *(continued)*

Parameter	Description
SYMREBOOT=*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 command-line client features" on page 816. **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 3 only. They do not apply to clients that run Windows Vista, or Windows 7 or later, except for the WSCAVUPTODATE property.

Windows Security Center was renamed to Action Center in Windows 7/8 and Security and Maintenance in Windows 10.

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 Windows 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 SYMREBOOT=ReallySuppress /qn /l*v c:\temp\msi.log`
Silently install the Symantec Endpoint Protection client with Virus and Spyware Protection, and with intrusion prevention and firewall. Force a computer restart, and create a verbose log file.	`msiexec /I SEP.msi ADDLOCAL=Core,SAVMain,OutlookSnapin, Pop3Smtp,ITPMain,Firewall SYMREBOOT=Force /qn /l*v c:\temp\msi.log`

Installing Windows clients with Microsoft SCCM/SMS

You can use Microsoft System Center Configuration Manager (SCCM) to install Symantec client software. We assume that system administrators who use SCCM have previously installed software with SCCM. As a result, we assume that you do not need detailed information about installing Symantec client software with SCCM.

Note: This topic also applies to Microsoft Systems Management Server (SMS).

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 SCCM/SMS packages launch Setup.exe rather than the MSI directly. This method enables installer logging. Use the custom package creation feature in SCCM/SMS to create custom packages instead of the package wizard feature.

Warning: You should use a managed client installation package that you exported from Symantec Endpoint Protection Manager. If you use the client installation packages from the product download or the installation file, you deploy unmanaged clients. Unmanaged clients install with default settings and do not communicate with a management server.

See "Installing Symantec Endpoint Protection clients with Save Package" on page 53.

Table B-7 Process for installing the client using Microsoft System Center Configuration Manager / Systems Management Server

Step	Description
Step 1	Export a managed client installation package from Symantec Endpoint Protection Manager that contains the software and policies to install on your client computers. By default, a managed client installation package contains a file named Sylink.xml, which identifies the server that manages the clients.
Step 2	Create a source directory and copy the Symantec client installation package into that source directory. For example, you would create a source directory and copy the Setup.exe file that you exported from Symantec Endpoint Protection Manager.
Step 3	In SCCM/SMS, create a custom 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 SCCM/SMS, see the Microsoft documentation that is appropriate for your version.

Installing Windows clients with an Active Directory Group Policy Object (GPO)

You can install the Windows client by using a Windows Active Directory Group Policy Object. The procedures assume that you have installed this software and use Windows Active Directory to install client software with an Active Directory Group Policy Object.

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 813.

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
```

Warning: You should use a managed client installation package that you exported from Symantec Endpoint Protection Manager. If you use the client installation packages from the product download or the installation file, you deploy unmanaged clients. Unmanaged clients install with default settings and do not communicate with a management server.

See "Installing Symantec Endpoint Protection clients with Save Package" on page 53.

Table B-8 Steps for installing the client software by using Active Directory Group Policy Object

Step	Action
Step 1	Export the managed client installation package with the option **Separate files (required for .MSI)**. See "Installing Symantec Endpoint Protection clients with Save Package" on page 53.
Step 2	Stage the folder of installation files. For example, copy the managed client installation package into a shared folder on which you have set the correct permissions to allow access.
Step 3	Create a GPO software distribution. You should also test GPO installation with a small number of computers before the production deployment. If you do not configure DNS properly, GPO installations can take an hour or more. See "Creating a GPO software distribution" on page 823.
Step 4	Add computers to the organizational unit. See "Adding computers to an organizational unit to install software" on page 825.

See "Uninstalling client software with an Active Directory Group Policy Object" on page 827.

Creating a GPO software distribution

If you use Microsoft Active Directory in your environment, you can use a GPO to deploy the Symantec Endpoint Protection client package to Windows computers. You create a software distribution then configure a GPO administrative template for the software packages.

This process assumes that you have installed Microsoft's Group Policy Management Console with Service Pack 1 or later. The Windows interface may be slightly different depending on the version of Windows you use.

This process also assumes that you have computers in the Computers group or some other group to which you want to install client software. Optionally, you can drag these computers into a new group that you create.

See "Installing Windows clients with an Active Directory Group Policy Object (GPO)" on page 822.

To create a GPO software distribution

1. On the Windows Taskbar, click **Start > All 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, select a target organizational unit (OU) under the appropriate domain.

   You can also create a new OU for testing or other purposes. See Active Directory documentation by Microsoft for more information on how to create a new OU.
4. In the **Group Policy Management** window, in the console tree, right-click the organizational unit that you chose or created, and then click **Create and Link a GPO Here**.

   You may need to refresh the domain to see a new OU.
5. In the **New GPO** dialog box, in the Name box, type a name for your GPO, and then click **OK**.
6. In the right pane, right-click the GPO that you created, and then click **Edit**.
7. In the **Group Policy Object Editor** window, in the left pane, under **Computer Configuration**, expand **Software Settings**.
8. Right-click **Software installation**, and then click **New > Package**.
9. 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`
10. Click **Open**.
11. 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 administrative templates for the software 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**

Note: If you enabled User Account Control (UAC) on the client computers, you must also enable **Computer Configuration > Administrative Templates > Windows Components > Windows Installer > Always install with elevated privileges** to install Symantec client software with a GPO. You set these options to allow all Windows users to install Symantec client software.

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**.

Adding computers to an organizational unit to install software

You can add computers to an organizational unit to which Symantec Endpoint Protection installs by GPO. 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 following process contains the commands that you can run on the client computers to update the policy on demand.

See "Installing Windows clients with an Active Directory Group Policy Object (GPO)" on page 822.

To add computers to the organizational unit to install software

1. On the Windows Taskbar, click **Start > All 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 chose for GPO installation.

   Computers first appear in the **Computers** organizational unit.

3 Drag and drop the computers into the organization unit that you chose or created for the installation.

4 Close the **Active Directory Users and Computers** window.

To update the GPO on demand on the client computers

1 To quickly apply the changes to the client computers, open a command prompt on the client computers.

2 Type **gpupdate**, and then press **Enter**.

When complete, the command prompt window displays a message to let you know the policy update completed successfully. If an error message displays, follow the on-screen instructions for more information.

3 Close the command prompt window.

Copying a Sylink.xml file to make a managed installation package

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 install the client from the installation file you get from Symantec, you install unmanaged clients. However, you can copy the Sylink.xml file to this folder before installation to install managed clients.

Note: Packages that are exported with the Symantec Endpoint Protection Manager console are managed and already include a Sylink.xml file. To export a new managed package that you can deploy with a Group Policy Object, use the Client Deployment Wizard. Click **Save Package**, and check **Separate Files (required for .MSI)** when prompted.

See "Installing Symantec Endpoint Protection clients with Save Package" on page 53.

To copy a Sylink.xml file to the product installation files to make a managed installation package

1 From Symantec Endpoint Protection Manager, export the Sylink.xml file from the correct client group and copy it to your computer.

Note: You should create at least one new group with the management console before you export the Sylink.xml file. If you do not, the clients appear in the Default group.

See "Adding a group" on page 237.

See "Exporting the client-server communications file (Sylink.xml) manually" on page 174.

2 Copy the installation folder from the installation file you download to a folder on your computer. The folder `SEP` contains the 32-bit client, and the folder `SEPx64` contains the 64-bit client.

You can also use the installation folder for an unmanaged client package that you previously exported as separate files.

3 Copy Sylink.xml to the installation folder. Replace the existing Sylink.xml file when prompted.

Uninstalling client software with an Active Directory Group Policy Object

You can uninstall the client software that you installed with Active Directory.

See "Uninstalling the Symantec Endpoint Protection client for Windows" on page 132.

To uninstall client software with an Active Directory Group Policy Object

1 On the Windows Taskbar, click **Start > All Programs > Administrative Tools > Group Policy Management**.

The version of Windows that you use may display **Programs** instead of **All 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.

Appendix C

Command-line options for the Windows client

This appendix includes the following topics:

Windows commands for the Endpoint Protection client service `smc`

You can run the Windows client service using the smc (or smc.exe) command-line interface. You can use the `smc` command in a script that runs the client remotely. For example, you may need to stop the client to install an application on multiple clients. You can then use the script to stop and restart all clients at one time.

The client service must be running for you to use the command-line parameters, with the exception of `smc -start` parameter. The command-line parameters are not case-sensitive. For some parameters, you may need the password. The client does not support UNC paths.

See "To run Windows commands using the `smc` command-line interface" on page 835.

See "`smc.exe` command error codes" on page 835.

Table C-1 `smc` parameters

Parameter	Description	Applies to
`smc -start` *	Starts the client service. Returns 0, -1	All supported versions

Table C-1 `smc` parameters *(continued)*

Parameter	Description	Applies to
`smc -stop` *†	Stops the client service and unloads it from memory. Returns 0, -1	All supported versions
`smc -checkinstallation`	Checks whether the `smc` client service is installed. Returns 0, -3	All supported versions
`smc -checkrunning`	Checks whether the `smc` client service is running. Returns 0, -4	All supported versions
`smc -cloudmanaged` *path_to_* `sep_setup.exe`	Moves a cloud-managed device to another cloud domain or tenant. Moves a client computer managed by Symantec Endpoint Protection Manager to be managed by the cloud console. Requires the `sep_setup.exe` installation file for the destination cloud domain/tenant. You download this file from the cloud console. Using smc to change a device's tenant or domain	As of 14.2 RU1
`smc -enable -ntp` `smc -disable -ntp` †	Enables/disables the Symantec Endpoint Protection firewall and Intrusion Prevention system.	All supported versions Password requirement for `-disable` as of 14.2 RU1
`smc -enable -mem` * `smc -disable -mem` *	Enables/disables the Symantec Endpoint Protection Memory Exploit Mitigation system.	As of version 14 MP1
`smc -dismissgui`	Closes the client user interface. The client still runs and protects the client computer. Returns 0	All supported versions

Table C-1 `smc` parameters *(continued)*

Parameter	Description	Applies to
`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	All supported versions

`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
		All supported versions

Table C-1 `smc` parameters *(continued)*

Parameter	Description	Applies to
`smc -exportadvrule` *†	Exports the client's firewall rules to an .xml 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.xml` Returns 0, -1, -5, -6 When you import configuration files and firewall rules, note that the following rule applies: ■ You cannot import configuration files or firewall rule files directly from a mapped network drive.	All supported versions

Table C-1 `smc` parameters *(continued)*

Parameter	Description	Applies to
`smc -importadvrule` *†	Imports firewall rules to the client. The rules you import overwrite any existing rules. You can import the following: ■ Rules in .xml format that you exported through `smc -exportadvrule` ■ Rules in .sar format that you exported through the client user interface You can only import firewall rules if the client is unmanaged, or if the managed client is in client control mode or mixed mode. The managed client ignores these rules in server control mode. To import firewall rules, you import an .xml or .sar file. For example, you can type the following command: `smc -importadvrule C:\myrules.xml` An entry is added to the System log after you import the rules. Returns 0, -1, -5, -6 To append rules instead of overwriting them, use **Import rule** from the within client user interface. See "Preventing and allowing users to change the client's user interface" on page 257.	All supported versions
`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	All supported versions
`smc -importsylink` †	Imports the client communications file (sylink.exe).	All supported versions

Table C-1 `smc` parameters *(continued)*

Parameter	Description	Applies to
`smc -enable -wss` `smc -disable -wss`	Enables or disables WSS Traffic Redirection.	As of version 14.0.1 MP1
`smc -p [password ]`†	Used with a command that requires a password, where [password] is the required password. For example: `smc -p [password] -importconfig`	All supported versions
`smc -report`	Creates a dump file (.dmp) that includes crashes and logical errors that occurred on the client. The file is sent automatically to Symantec Technical Support. Contact Technical Support to ask for help in diagnosing the error. You can find the dump file at the following location: *`SEP_Install`*`\Data\LocalDumps` Where *SEP_Install* is the installation folder. By default, this is C:\Program Files (x86)\Symantec\Symantec Endpoint Protection*version*.	As of version 14
`smc -runhi`	Runs a Host Integrity check. Returns 0	All supported versions
`smc -showgui`	Displays the client user interface. Returns 0	All supported versions
`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	All supported versions

* Parameters that only members of the Administrators group can use if the following conditions are met:

- The client runs Windows Vista or Windows Server 2008, and users are members of the Windows Administrators group.

If the client runs Windows Vista and the User Account Control is enabled, the user automatically becomes a member of both the Administrators group and Users group.

† Parameters that need a password. You password-protect the client in Symantec Endpoint Protection Manager.

To run Windows commands using the `smc` command-line interface

1. On the client computer, click **Start > Run**, and then type **cmd**.
2. In the MS-DOS prompt, do one of the following tasks:
   - If the parameter does not need a password, type:

     smc -parameter

     Where *parameter* is a parameter.
   - If the parameter needs a password, enter the following:
     - ***smc -p password -parameter***

     For example: `smc -p password -exportconfig c:\profile.xml`

Note: You must type the installation path to the `smc` service before the command. For example, on a 64-bit Windows system on which Symantec Endpoint Protection is installed to the default location, type:

```
C:\Program Files (x86)\Symantec\Symantec Endpoint Protection\smc.exe
```

See "Password-protecting the Symantec Endpoint Protection client" on page 260.

`smc.exe` command error codes

Table C-2 displays the error codes that the `smc.exe` command returns when the required parameters are invalid or missing.

Table C-2 `smc.exe` command 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.

Table C-2 `smc.exe` command error codes *(continued)*

Error code	Description
-3	`smc` client service is not installed.
-4	`smc` client service is not running.
-5	Invalid input file. For example, the `importconfig`, `exportconfig`, `updateconfig`, `importadv`, `exportadvrule`, and `exportlog` parameters require the correct path name and file name.
-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).

See "Windows commands for the Endpoint Protection client service `smc`" on page 829.

Appendix D

Symantec Endpoint Protection tools

This appendix includes the following topics:

What are the tools included with Symantec Endpoint Protection?

This article describes the tools that are included with Symantec Endpoint Protection and what you use the tools for.

Tools that are located on the installation file on MySymantec

Tools that are installed with Symantec Endpoint Protection Manager

Tools that are located on the installation file on MySymantec

The following tools and documentation are located in the \Tools folder of the Symantec Endpoint Protection installation file that you download from MySymantec.

- ApacheReverseProxy (12.1.4 and later)
- CentralQ (12.1.6 and earlier)
- CleanWipe
- ContentDistributionMonitor (SEPMMonitor)
- Deception (14.0.1)
- DeviceInfo (14), DevViewer
- Integration (WebServicesDocumentation)
- ITAnalytics

- JAWS
- LiveUpdate Administrator (12.1.4 and earlier)
- No Support > MoveClient
- No Support > Qextract
- No Support > SEPprep (12.1.6 and earlier)
- OfflineImageScanner (12.1.6 and earlier)
- PushDeploymentWizard
- SylinkDrop
- SymDiag (SymHelp)
- Virtualization
- WebServicesDocumentation (Integration)

Product guides for all versions of Symantec Endpoint Protection

ApacheReverseProxy (12.1.4 and later)

This tool sets up the Apache webserver in Symantec Endpoint Protection Manager to allow Mac clients and Linux clients to download LiveUpdate content through the web server. The Apache webserver works with the Symantec Endpoint Protection Manager to download and cache the LiveUpdate content for Mac and Linux clients locally whenever new content is published.

This tool is appropriate for networks with a smaller number of clients.

CentralQ (12.1.6 and earlier)

Symantec Endpoint Protection can automatically forward the quarantine packages that contain the infected files and related side effects from a local quarantine to the Central Quarantine. You can gather forensic information more easily by using Central Quarantine. This tool lets you retrieve a sample from an infected computer without having to directly access that computer.

Use the Quarantine Server in a Symantec Endpoint Protection environment in the following cases:

- To receive suspected threat samples from Symantec Endpoint Protection clients.
- To submit these samples to Security Response automatically.
- To download the rapid release definitions that are specific to the suspected threats that have been submitted only to the Quarantine Server. These definitions are not pushed to the Symantec Endpoint Protection clients where the threat originated from.
  Rapid Release Virus Definitions

For more information, see: Best Practices for using Quarantine Server in a Symantec Endpoint Protection environment

CleanWipe

CleanWipe uninstalls the Symantec Endpoint Protection product. Only use CleanWipe as a last resort after you have unsuccessfully tried other uninstallation methods, such as the Windows Control Panel.

Uninstall Symantec Endpoint Protection

You can also find this tool in the following location (64-bit): C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\Tools

ContentDistributionMonitor (SEPMMonitor)

The ContentDistributionMonitor tool helps you manage and monitor multiple Group Update Providers (GUPs) in your environment. The tool presents a graphical display of the GUPs' health and content distribution status.

In 12.1.6 and earlier, `ContentDistributionMonitor` was named `SEPMMonitor`. In 12.1.5 and earlier, `ContentDistributionMonitor` was in the `NoSupport` folder.

See: Symantec Endpoint Protection Content Distribution Monitor tool

Deception (14.0.1)

Deception is used to detect adversary activity at the endpoint using "deceptors." The underlying assumption with this approach is that the attacker has already breached the primary defenses of the network and performs reconnaissance in the environment. The attacker looks to find critical assets, like a domain controller or database credentials.

DeviceInfo (14), DevViewer

DeviceInfo (for Mac; as of version 14) and DevViewer (for Windows) obtains the device vendor, model, or serial number for a specific device. You add this information to the **Hardware Devices** list. You can then add the device ID to a Device Control policy to allow or block a device on client computers.

See “Adding a hardware device to the Hardware Devices list” on page 542.

Block or allow devices in Endpoint Protection

Integration (WebServicesDocumentation)

As of version 14, the Integration folder was renamed to `WebServicesDocumentation`.

WebServicesDocumentation (Integration)

ITAnalytics

The IT Analytics software expands the built-in reporting that Symantec Endpoint Protection offers by enabling you to create custom reports and custom queries. It brings multi-dimensional analysis and graphical reporting features from the data that is contained within the Symantec Endpoint Protection Manager databases. This functionality allows you to explore data on your own, without advanced knowledge of databases or third-party reporting tools.

JAWS

The JAWS screen reader program and a set of scripts make it easier to read the Symantec Endpoint Protection menus and dialogs. JAWS is an assistive technology that provides compliance with Section 508 product accessibility.

LiveUpdate Administrator (12.1.4 and earlier)

Symantec LiveUpdate Administrator is a standalone web application that is separate from Symantec Endpoint Protection. LiveUpdate Administrator mirrors the content of the public LiveUpdate servers and then offers the content to Symantec products internally through a built-in web server.

LiveUpdate Administrator is an optional component for Symantec Endpoint Protection and is not required to update the Symantec Endpoint Protection clients. By default, the Symantec Endpoint Protection Manager uses the LiveUpdate technology rather than LiveUpdate Administrator to download contents directly from the Symantec public LiveUpdate servers.

You may want to use LiveUpdate Administrator in some circumstances. For example, you may need to download content to a large number of non-Windows clients or to clients if Symantec Endpoint Protection Manager cannot download the content. Therefore, you can install a LiveUpdate Administrator server and then configure the Symantec Endpoint Protection Manager to download from it.

When to use LiveUpdate Administrator

To download LiveUpdate Administrator and the documentation, see: Download LiveUpdate Administrator (LUA)

LiveUpdate Administrator 2.3.x Release Notes

No Support > MoveClient

`MoveClient` is a Visual Basic script that moves clients from one Symantec Endpoint Protection Manager group to another group based on the client's host name, user name, IP address, or operating system. It also can switch clients from user mode to computer mode and vice versa.

See “Switching a Windows client between user mode and computer mode” on page 254.

No Support > Qextract

`Qextract` extracts and restores files from the client's local quarantine. You might need this tool if the client quarantines a file that you determine is a false positive.

No Support > SEPprep (12.1.6 and earlier)

SEPprep is an unsupported tool that uninstalls competitors' antivirus products automatically. SEPprep also uninstalls Symantec Norton™ products if you want to migrate from Norton to Symantec Endpoint Protection.

You can package SEPprep in a script which uninstalls the competitor's product, and then launches the Symantec Endpoint Protection installer automatically and silently.

Instead of SEPprep, use the Client Deployment Wizard to uninstall competitors' products. On the **Client Install Settings** tab in the wizard, click **Automatically uninstall existing third-party security software**.

See "Configuring client packages to uninstall existing security software" on page 124.

Uninstall third-party security software using SEPprep

For a list of products that the Client Deployment Wizard uninstalls, see:

Third-party security software removal in Endpoint Protection 12.1

SEPprep does not uninstall any Symantec products. However, as of version 14, CleanWipe is built into the Client Deployment Wizard to remove other Symantec products, including the Symantec Endpoint Protection client.

OfflineImageScanner (12.1.6 and earlier)

This tool scans and detects threats in offline VMware virtual disks (.vmdk files).

About the Symantec Offline Image Scanner tool

PushDeploymentWizard

You use the Push Deployment Wizard to deploy the Symantec Endpoint Protection client installation package to target computers. Push Deployment Wizard is the same as the Client Deployment Wizard in Symantec Endpoint Protection Manager. You typically use it to deploy to smaller groups of computers or remote computers.

For more information, see: Overview of the Push Deployment Wizard in Symantec Endpoint Protection

SEPIntegrationComponent (12.1.5 and earlier)

The Symantec Endpoint Integration Component (SEPIC) combines Symantec Endpoint Protection with other Symantec Management Platform solutions using a single, web-based Symantec Management Console. You use SEPIC to inventory computers, update patches,

deliver software, and deploy new computers. You can also back up and restore your systems and data, manage DLP agents, and manage Symantec Endpoint Protection clients.

SylinkDrop

The Sylink.xml file includes communication settings between the Windows client or Mac client and a Symantec Endpoint Protection Manager. If the clients have lost the communication with Symantec Endpoint Protection Manager, use the SylinkDrop tool to automatically replace the existing Sylink.xml file with a new Sylink.xml file on the client computer.

Replacing the Sylink.xml file does the following tasks:

- Converts an unmanaged client to a managed client.
- 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.

You can also use this tool for Windows clients only; the tool is located in the following location (64-bit): `C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\Tools`

See "Restoring client-server communication settings by using the SylinkDrop tool" on page 772.

SymDiag (SymHelp)

As of version 14, the SymHelp tool was renamed as Symantec Diagnostic (SymDiag).

`SymDiag` is a multi-product diagnostic tool that identifies common issues, gathers data for support-assisted troubleshooting, and provides links to other customer self-help and support resources. `SymDiag` also provides licensing and maintenance status for some Symantec products as well as the Threat Analysis Scan, which helps to find potential malware.

Virtualization

The virtualization tools improve scan performance for the clients that are installed in virtual desktop infrastructure (VDI) environments.

- **SecurityVirtualAppliance (12.1.6 and earlier)**
  The Symantec Security Virtual Appliance contains the vShield-enabled Shared Insight Cache for VMware vShield infrastructures.
  What do I need to do to install a Security Virtual Appliance?
  Installing a Symantec Endpoint Protection Security Virtual Appliance
- **SharedInsightCache**

The Shared Insight Cache tool improves scan performance in virtualized environments by not scanning the files that a Symantec Endpoint Protection client has determined are clean. When the client scans a file for threats and determines it is clean, the client submits information about the file to Shared Insight Cache.

When another client subsequently attempts to scan the same file, that client can query Shared Insight Cache to determine if the file is clean. If the file is clean, the client does not scan that particular file. If the file is not clean, the client scans the file for viruses and submits those results to Shared Insight Cache.

Shared Insight Cache is a web service that runs independently of the client. However, Symantec Endpoint Protection must be configured to specify the location of Shared Insight Cache so that the clients can communicate with it. Shared Insight Cache communicates with the clients through HTTP or HTTPS. The client's HTTP connection is maintained until the scan is finished.

Installation and Configuration of SEP Shared Insight Cache

- **Virtual Image Exception**
  To increase performance and security in a VDI environment, a common practice is to leverage base images to build virtual machine sessions as needed. The Symantec Virtual Image Exception tool lets Symantec Endpoint Protection clients bypass scanning base image files for threats, which reduces the resource load on disk I/O. It also improves CPU scanning process performance in a VDI environment.
  About the Symantec Virtual Image Exception tool

WebServicesDocumentation (Integration)

In 12.1.6 and earlier, this tool is located in the \Tools\Integration folder.

Symantec Endpoint Protection includes a set of public APIs in the form of web services to provide support for remote monitoring and management (RMM) applications. The web services provide functions on the client and on the management server. All calls to Symantec Endpoint Protection web services are authenticated using `OAuth` and allow access only by authorized Symantec Endpoint Protection administrators. Developers use these APIs to integrate their company's third-party network security solution with the Symantec Endpoint Protection management server and client.

Provides the support for remote management and remote monitoring. Remote management is provided by means of public APIs in the form of web services that let you integrate your third-party solution or custom console with basic client and management server functionality. Remote monitoring is provided by means of publicly supported registry keys and Windows event logging.

Web services for remote management can do the following tasks:

- Reports the license status and content status on the management server by web service calls, in addition to reporting the license status to the Windows Event Log.
- Issues commands to the client, such as Update, Update and Scan, and Restart.

- Manages the policies that are delivered to the client. Policies can be imported from another management server, and they can be assigned to groups or locations at another management server.

Tools that are installed with Symantec Endpoint Protection Manager

The following tools are installed with the Symantec Endpoint Protection Manager in the following default location: `C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\Tools`.

- CleanWipe
- CollectLog
- Database Validator
- SetSQLServerTLSEncryption (14)
- SylinkDrop
- Symantec Endpoint Protection Manager API reference (14)

CollectLog

CollectLog.cmd places the Symantec Endpoint Protection Manager logs in a compressed .zip file. You send the .zip file to Symantec Support or another administrator for troubleshooting purposes.

You find this tool in the following location (64-bit): C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\Tools

Database Validator

You use dbvalidator.bat to help Support diagnose a problem with the database that Symantec Endpoint Protection Manager runs.

You find this tool in the following location (64-bit): C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\Tools

SetSQLServerTLSEncryption (14)

Symantec Endpoint Protection Manager communicates with the Microsoft SQL Server over an encrypted channel by default. This tool lets you disable or enable TLS encryption between the management server and the Microsoft SQL Server communication. As of version 14, it can be used with the management server installations that are configured to use the Microsoft SQL Server database.

This tool is installed with Symantec Endpoint Protection Manager in the following location (64-bit): C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\Tools

Symantec Endpoint Protection Manager API reference (14)

Symantec Endpoint Protection Manager includes a set of REST APIs that connect to and perform Symantec Endpoint Protection Manager operations from Endpoint Detection and Response (EDR). You use the APIs if you do not have access to Symantec Endpoint Protection Manager. The documentation is located in the following places:

- On the Symantec Endpoint Protection Manager server at the following address, where *SEPM-IP* is the IP address of the Symantec Endpoint Protection Manager server:
  https://*SEPM-IP*:8446/sepm/restapidocs.html
  IP address includes IPv4 and IPv6. You must enclose the IPv6 address with square brackets: **http://[*SEPMServer*]:*port number***
- Product guides for all versions of Symantec Endpoint Protection

Appendix E

Command-line options for the Virtual Image Exception tool

This appendix includes the following topics:

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 Virtual Image Exception tool uses the hashes to exclude local files from future scans. The clients compute file hashes separately to send to the Shared Insight Cache to store scan results. 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.

Index

D

E

F

G

H

I

J

L

M

N

O

P

Q

R

S

T

U

V

W