

Symantec™ Endpoint Protection 12.1.6 Installation and Administration Guide



Symantec Endpoint Protection Installation and Administration Guide

Product version 12.1.6

Documentation version: 2

This document was last updated on: June 06, 2015

Legal Notice

Copyright © 2015 Symantec Corporation. All rights reserved.

Symantec, the Symantec Logo, the Checkmark Logo, LiveUpdate, and TruScan are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

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

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

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

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

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

<http://www.symantec.com>

Technical Support

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

Symantec's support offerings include the following:

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

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

www.symantec.com/business/support/

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

Contacting Technical Support

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

www.symantec.com/business/support/

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

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

- Product release level
- Hardware information

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

Licensing and registration

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

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

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

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

Support agreement resources

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

Asia-Pacific and Japan customercare_apj@symantec.com

Europe, Middle-East, and Africa semea@symantec.com

North America and Latin America supportsolutions@symantec.com

Contents

Technical Support	4	
Chapter 1	Introducing Symantec Endpoint Protection	29
	What is Symantec Endpoint Protection?	29
	What's new in Symantec Endpoint Protection 12.1.6	30
	How Symantec Endpoint Protection uses layers to protect computers	36
	How does Symantec Endpoint Protection enforce compliance?	38
Section 1	Installing Symantec Endpoint Protection	40
Chapter 2	Planning the installation	41
	Getting up and running on Symantec Endpoint Protection for the first time	41
	Components of Symantec Endpoint Protection	50
	Optional components for Symantec Endpoint Protection	51
	System requirements for Symantec Endpoint Protection	52
	System requirements for Symantec Endpoint Protection Manager	53
	System requirements for the Symantec Endpoint Protection client for Windows	55
	System requirements for the Symantec Endpoint Protection client for Windows Embedded	56
	System requirements for the Symantec Endpoint Protection client for Mac	57
	System requirements for the Symantec Endpoint Protection client for Linux	58
	Internationalization requirements	59
	Product license requirements	61
	Supported virtual installations and virtualization products	62
	Network architecture considerations	64
	About choosing a database type	65
	About basic management server settings	65

	Management server ports	67
	About SQL Server configuration settings	68
	About SQL Server database authentication modes	72
Chapter 3	Installing Symantec Endpoint Protection Manager	74
	Installing Symantec Endpoint Protection Manager	74
	Configuring Symantec Endpoint Protection Manager during installation	76
	Uninstalling Symantec Endpoint Protection Manager	77
	Logging on to the Symantec Endpoint Protection Manager console	78
	About accepting the self-signed server certificate for Symantec Endpoint Protection Manager	81
	Displaying a message for administrators to see before logging on to the Symantec Endpoint Protection Manager console	82
	Displaying the Remember my user name and Remember my password check boxes on the logon screen	82
	Granting or blocking access to remote Symantec Endpoint Protection Manager consoles	83
	Configuring an administrator's account to lock after too many logon attempts	84
	Changing the time period for staying logged on to the console	85
	What you can do from the console	86
	What do I do after I install the management server?	88
Chapter 4	Managing product licenses	92
	Licensing Symantec Endpoint Protection	92
	About the trial license	94
	About purchasing licenses	95
	Activating or importing your Symantec Endpoint Protection 12.1.x product license	96
	Required licensing contact information	99
	About the Symantec Licensing Portal	100
	About product upgrades and licenses	100
	About renewing your Symantec Endpoint Protection license	101
	Checking the license status in Symantec Endpoint Protection Manager	101
	About the licensing enforcement rules	102
	Backing up your license files	103
	Recovering a deleted license	103

	Purging obsolete clients from the database to make more licenses available	104
	About multi-year licenses	105
	Licensing an unmanaged Windows client	105
Chapter 5	Installing the Symantec Endpoint Protection client	107
	Preparing for client installation	108
	Preparing Windows and Mac computers for remote deployment	111
	About the communication ports that Symantec Endpoint Protection uses	113
	About reduced-size client installation packages	114
	About client installation methods	115
	Which features should you install on the client?	117
	Installing clients with Web Link and Email	118
	Installing clients with Remote Push	120
	Installing clients with Save Package	122
	Exporting client installation packages	124
	About the Windows client installation settings	126
	Configuring Windows client installation feature sets	127
	Configuring client packages to uninstall existing third-party security software	127
	Restarting the client computers from Symantec Endpoint Protection Manager	129
	Installing the Symantec Endpoint Protection client for Mac	130
	Installing the Symantec Endpoint Protection client for Linux	132
	About managed and unmanaged clients	134
	Download an unmanaged Symantec Endpoint Protection client installation package	135
	Installing an unmanaged Windows client	136
	Uninstalling the Symantec Endpoint Protection client for Windows	137
	Uninstalling the Symantec Endpoint Protection client for Mac	138
	Uninstalling the Symantec Endpoint Protection client for Linux	139
	Managing client installation packages	140
	Adding client installation package updates	142
Chapter 6	Upgrading Symantec Endpoint Protection	144
	Upgrading to a new release	145
	Upgrade resources for Symantec Endpoint Protection 12.1.x	147
	Supported upgrade paths to Symantec Endpoint Protection	148

Increasing Symantec Endpoint Protection Manager available disk space before upgrading to version 12.1.x	150
Upgrading a management server	152
Upgrading an environment that uses multiple embedded databases and management servers	154
Turning off replication before an upgrade from Symantec Endpoint Protection 11.0	155
Turning on replication after an upgrade from Symantec Endpoint Protection 11.0	155
Stopping and starting the management server service	156
About upgrading client software	157
Upgrading Windows clients by using AutoUpgrade in Symantec Endpoint Protection	158
Updating client software with a LiveUpdate Settings policy	160
Upgrading Group Update Providers	161
Enabling Symantec Network Access Control functionality in Symantec Endpoint Protection	161
Enabling Symantec Network Access Control in Symantec Endpoint Protection Manager	162

Section 2 Managing client-server communication and updating content 164

Chapter 7 Managing client-server communication	165
Managing the client-server connection	165
How to determine whether the client is connected in the console	167
How to determine whether the client computer is connected and protected	169
How the client computer and the management server communicate	169
Configuring push mode or pull mode to update client policies and content	170
Using the policy serial number to check client-server communication	172
Why do I need to replace the client-server communications file on the client computer?	173
How do I replace the client-server communications file on the client computer?	174
Restoring client-server communications with Communication Update Package Deployment	175

Exporting the client-server communications file (Sylink.xml) manually	176
Importing client-server communication settings into the Windows client	178
Importing client-server communication settings into the Linux client	179
Chapter 8	
Updating content on the clients	180
Managing content updates	181
Choose a distribution method to update content on clients	182
Choose a distribution method to update content on clients based on the platform	187
Configuring a site to download content updates	189
Configuring the LiveUpdate download schedule for Symantec Endpoint Protection Manager	192
Running LiveUpdate and downloading content to Symantec Endpoint Protection Manager immediately	193
Mitigating network overloads for client update requests	193
Checking LiveUpdate server activity	194
Configuring Symantec Endpoint Protection Manager to connect to a proxy server to access the Internet and download content from Symantec LiveUpdate	195
Specifying a proxy server that clients use to communicate to Symantec LiveUpdate or an internal LiveUpdate server	195
Configuring the types of content used to update client computers	196
About the types of content that LiveUpdate can provide	197
Configuring the LiveUpdate download schedule for client computers	202
Configuring the amount of control that users have over LiveUpdate	204
Configuring the content revisions that clients use	205
About randomization of simultaneous content downloads	206
Randomizing content downloads from the default management server or a Group Update Provider	207
Randomizing content downloads from a LiveUpdate server	208
Configuring client updates to run when client computers are idle	209
Configuring client updates to run when definitions are old or the computer has been disconnected	210
Setting up an external LiveUpdate server for Symantec Endpoint Protection clients	210
Setting up an internal LiveUpdate server for Symantec Endpoint Protection clients	211

	Using Group Update Providers to distribute content to clients	215
	About the types of Group Update Providers	216
	About the effects of configuring more than one type of Group Update Provider in your network	220
	About configuring rules for multiple Group Update Providers	222
	Configuring Group Update Providers	223
	Searching for the clients that act as Group Update Providers	226
	Using Intelligent Updater files to update content on Windows computers	227
	Using third-party distribution tools to update client computers	228
	Configuring a LiveUpdate Settings policy to allow third-party content distribution to managed clients	229
	Preparing unmanaged clients to receive updates from third-party distribution tools	230
	Distributing the content using third-party distribution tools	231
Section 3	Managing groups, clients, and administrators	235
Chapter 9	Managing groups of client computers	236
	Managing groups of clients	236
	How you can structure groups	238
	Adding a group	239
	Importing existing groups and computers from an Active Directory or an LDAP server	240
	About importing organizational units from the directory server	241
	Connecting Symantec Endpoint Protection Manager to a directory server	242
	Connecting to a directory server on a replicated site	243
	Importing organizational units from a directory server	244
	Searching for and importing specific accounts from a directory server	245
	Assigning clients to groups before you install the client software	246
	Disabling and enabling a group's inheritance	247
	Blocking client computers from being added to groups	248
	Moving a client computer to another group	248
Chapter 10	Managing clients	250
	Managing client computers	250
	Viewing the protection status of clients and client computers	253

	Searching for the clients that do not have the client software installed	254
	Searching for information about client computers	255
	About enabling and disabling protection when you need to troubleshoot problems	256
	About commands that you can run on client computers	258
	Running commands on client computers from the console	261
	Ensuring that a client does not restart	263
	Switching a Windows client between user mode and computer mode	263
	Configuring a client to detect unmanaged devices	265
	About access to the client interface on Windows clients	266
	Locking and unlocking settings by changing the user control level	267
	Unlocking user interface settings on the client	270
	Collecting user information	272
	Password-protecting the client	273
Chapter 11	Managing remote clients	274
	Managing remote clients	274
	Managing locations for remote clients	276
	Enabling location awareness for a client	278
	Adding a location to a group	279
	Changing a default location	280
	Setting up Scenario One location awareness conditions	281
	Setting up Scenario Two location awareness conditions	283
	Configuring communication settings for a location	285
	About strengthening your security policies for remote clients	286
	Best practices for Firewall policy settings	287
	LiveUpdate policy settings for clients in different locations	288
	About turning on notifications for remote clients	288
	About customizing log management settings for remote clients	289
	About monitoring remote clients	289
Chapter 12	Managing administrator accounts and passwords	291
	Managing administrator accounts	291
	About administrator account roles and access rights	293
	Adding an administrator account	295
	Configuring the access rights for a limited administrator	296
	Changing the authentication method for administrator accounts	297
	Configuring the management server to authenticate administrators who use RSA SecurID to log on	298

	Authenticating administrators who use RSA SecurID to log on to the management server	300
	Best practices for testing whether a directory server authenticates an administrator account	300
	Changing the password for an administrator account	305
	Resetting a forgotten Symantec Endpoint Protection Manager password	306
	Displaying the Forgot your password? link so that administrators can reset lost passwords	307
	Enabling Symantec Endpoint Protection Manager logon passwords to never expire	308
Chapter 13	Managing domains	309
	About domains	309
	Adding a domain	311
	Switching to the current domain	311
Section 4	Managing security policies	313
Chapter 14	Using policies to manage security	314
	Manually updating policies on the client	315
	Performing the tasks that are common to all policies	315
	The types of security policies	318
	Adding a policy	320
	Editing a policy	321
	Copying and pasting a policy on the Policies page	322
	Copying and pasting a policy on the Clients page	322
	Assigning a policy to a group	323
	Replacing a policy	325
	Exporting and importing individual policies	326
	About shared and non-shared policies	327
	Converting a shared policy to a non-shared policy	328
	Withdrawing a policy from a group	329
	Locking and unlocking Virus and Spyware Protection policy settings	330
	Monitoring the applications and services that run on client computers	331
	Configuring the management server to collect information about the applications that the client computers run	332
	Searching for information about the applications that the computers run	333

Chapter 15	Managing firewall protection	336
	Managing firewall protection	336
	How a firewall works	337
	About the Symantec Endpoint Protection firewall	338
	Creating a firewall policy	339
	Enabling and disabling a firewall policy	342
	Automatically allowing communications for essential network services	343
	Configuring firewall settings for mixed control	344
	Automatically blocking connections to an attacking computer	345
	Detecting potential attacks and spoofing attempts	346
	Preventing stealth detection	347
	Disabling the Windows firewall	347
	Managing firewall rules	348
	About firewall server rules and client rules	350
	About the firewall rule, firewall setting, and intrusion prevention processing order	351
	About inherited firewall rules	352
	Changing the order of firewall rules	354
	How the firewall uses stateful inspection	355
	About firewall rule application triggers	356
	About firewall rule host triggers	360
	About firewall rule network services triggers	364
	About firewall rule network adapter triggers	365
	Setting up firewall rules	367
	Adding a new firewall rule	368
	Importing and exporting firewall rules	369
	Customizing firewall rules	370
Chapter 16	Managing intrusion prevention	380
	Managing intrusion prevention on client computers	380
	How intrusion prevention works	383
	About Symantec IPS signatures	384
	About custom IPS signatures	385
	Enabling or disabling network intrusion prevention or browser intrusion prevention	386
	Creating exceptions for IPS signatures	387
	Setting up a list of excluded computers	389
	Configuring client intrusion prevention notifications	390
	Managing custom intrusion prevention signatures	391
	Creating a custom IPS library	392
	Adding signatures to a custom IPS library	393

	Assigning multiple custom IPS libraries to a group	395
	Changing the order of custom IPS signatures	395
	Defining variables for custom IPS signatures	396
	Testing custom IPS signatures	397
Chapter 17	Managing Virus and Spyware Protection	398
	Preventing and handling virus and spyware attacks on client computers	399
	Remediating risks on the computers in your network	401
	Identifying the infected and at-risk computers	403
	Checking the scan action and rescanning the identified computers	404
	Managing scans on client computers	405
	About the types of scans and real-time protection	408
	About the types of Auto-Protect	410
	About virus and security risks	412
	About the files and folders that Symantec Endpoint Protection excludes from virus and spyware scans	414
	About the default Virus and Spyware Protection policy scan settings	417
	How Symantec Endpoint Protection handles detections of viruses and security risks	421
	How Symantec Endpoint Protection handles detections on Windows 8 computers	422
	Setting up scheduled scans that run on Windows computers	422
	Setting up scheduled scans that run on Mac computers	424
	Setting up scheduled scans that run on Linux computers	425
	Running on-demand scans on client computers	426
	Adjusting scans to improve computer performance	427
	Adjusting scans to increase protection on your client computers	430
	Managing Download Insight detections	432
	How Symantec Endpoint Protection uses reputation data to make decisions about files	436
	How Symantec Endpoint Protection policy features work together on Windows computers	437
	About submitting information about detections to Symantec Security Response	440
	About submissions throttling	441
	Enabling or disabling client submissions to Symantec Security Response	442
	Specifying a proxy server for client submissions and other external communications	444

Managing the Quarantine	445
Specifying a local Quarantine folder	446
Specifying when repaired files, backup files, and quarantined files are automatically deleted	447
Configuring clients to submit quarantined items to a Central Quarantine Server or Symantec Security Response	448
Configuring how the Quarantine handles the rescanning of files after new definitions arrive	448
Using the Risk log to delete quarantined files on your client computers	449
Managing the virus and spyware notifications that appear on client computers	450
About the pop-up notifications that appear on Windows 8 clients	452
Enabling or disabling Symantec Endpoint Protection pop-up notifications that appear on Windows 8 clients	453
Managing early launch anti-malware (ELAM) detections	453
Adjusting the Symantec Endpoint Protection early launch anti-malware (ELAM) options	455
Configuring a site to use a private Insight server for reputation queries	456
Configuring client groups to use private servers for reputation queries and submissions	457

Chapter 18

Customizing scans	460
Customizing the virus and spyware scans that run on Windows computers	461
Customizing the virus and spyware scans that run on Mac computers	462
Customizing the virus and spyware scans that run on Linux computers	463
Customizing Auto-Protect for Windows clients	464
Customizing Auto-Protect for Mac clients	465
Customizing Auto-Protect for Linux clients	466
Customizing Auto-Protect for email scans on Windows computers	468
Customizing administrator-defined scans for clients that run on Windows computers	469
Customizing administrator-defined scans for clients that run on Mac computers	470
Customizing administrator-defined scans for clients that run on Linux computers	472

	Randomizing scans to improve computer performance in virtualized environments on Windows clients	473
	Modifying global scan settings for Windows clients	474
	Modifying miscellaneous settings for Virus and Spyware Protection on Windows computers	475
	Modifying miscellaneous settings for Virus and Spyware Protection on Linux computers	476
	Customizing Download Insight settings	477
	Changing the action that Symantec Endpoint Protection takes when it makes a detection	478
	Allowing users to view scan progress and interact with scans on Windows computers	480
	How Symantec Endpoint Protection interacts with Windows Security Center	482
Chapter 19	Managing SONAR	484
	About SONAR	484
	Managing SONAR	486
	Handling and preventing SONAR false positive detections	488
	Adjusting SONAR settings on your client computers	490
	Monitoring SONAR detection results to check for false positives	491
Chapter 20	Managing Tamper Protection	493
	About Tamper Protection	493
	Changing Tamper Protection settings	494
Chapter 21	Managing exceptions	495
	Managing exceptions in Symantec Endpoint Protection	495
	About exceptions in Symantec Endpoint Protection to Virus and Spyware scans	497
	Creating exceptions for Virus and Spyware scans	498
	Excluding a file or a folder from scans	503
	Excluding known risks from virus and spyware scans on Windows clients	505
	Excluding file extensions from virus and spyware scans on Windows clients and Linux clients	506
	Monitoring an application to create an exception for the application on Windows clients	507
	Specifying how Symantec Endpoint Protection handles monitored applications on Windows clients	507

	Excluding a trusted Web domain from scans on Windows clients	508
	Creating a Tamper Protection exception on Windows clients	509
	Creating an exception for an application that makes a DNS or host file change	510
	Restricting the types of exceptions that users can configure on client computers	511
	Creating exceptions from log events in Symantec Endpoint Protection Manager	511
Chapter 22	Testing security policies	514
	Testing Symantec Endpoint Protection Manager policies	514
	Testing a Virus and Spyware Protection policy	515
	Blocking a process from starting on client computers	516
	Preventing users from writing to the registry on client computers	517
	Preventing users from writing to a particular file	518
	Adding and testing a rule that blocks a DLL	519
	Adding and testing a rule that terminates a process	520
Section 5	Enforcing policies and meeting compliance requirements	522
Chapter 23	Managing application control, device control, and system lockdown	523
	About application and device control	523
	About Application and Device Control policies	525
	About the structure of an Application and Device Control policy	525
	Setting up application and device control	526
	Enabling a default application control rule set	528
	Creating custom application control rules	529
	Best practices for creating application control rules	531
	Typical application control rules	533
	Creating a custom rule set and adding rules	535
	Copying application rule sets or rules between Application and Device Control policies	536
	Applying a rule to specific applications and excluding applications from a rule	537
	Adding conditions and actions to a custom application control rule	539
	Testing application control rule sets	540
	Configuring system lockdown	541

Creating a file fingerprint list with checksum.exe	548
Importing or merging file fingerprint lists in Symantec Endpoint Protection Manager	550
Manually updating a file fingerprint list in Symantec Endpoint Protection Manager	551
Interaction between system lockdown and ATP: Endpoint blacklist rules	552
Creating an application name list to import into the system lockdown configuration	553
Automatically updating whitelists or blacklists for system lockdown	554
Setting up and testing the system lockdown configuration before you enable system lockdown	559
Running system lockdown in whitelist mode	561
Running system lockdown in blacklist mode	562
Testing selected items before you add or remove them when system lockdown is already enabled	564
Managing device control	565
About the hardware devices list	566
Obtaining a class ID or device ID	567
Adding a hardware device to the Hardware Devices list	568
Configuring device control	569

Chapter 24

Managing Host Integrity to enforce security policies	570
How Host Integrity works	571
Setting up Host Integrity	572
About Host Integrity requirements	574
Adding predefined requirements to a Host Integrity policy	575
Enabling and disabling Host Integrity requirements	576
Setting up remediation for a predefined Host Integrity requirement	576
Allowing users to delay or cancel Host Integrity remediation	577
Configuring the frequency of Host Integrity check settings	579
Allowing the Host Integrity check to pass if a requirement fails	579
Configuring notifications for Host Integrity checks	580
Creating a Quarantine policy for a failed Host Integrity check	581
Configuring peer-to-peer authentication for Host Integrity enforcement	582
Adding a custom requirement from a template	583
Writing a customized requirement script	584
About registry conditions	586

	Writing a custom requirement to run a script on the client	587
	Writing a custom requirement to set the timestamp of a file	588
	Writing a custom requirement to increment a registry DWORD value	589
	Creating a test Host Integrity policy with a custom requirement script	589
Section 6	Monitoring and reporting	592
Chapter 25	Monitoring protection with reports and logs	593
	Monitoring endpoint protection	593
	Viewing a daily or weekly status report	597
	Viewing system protection	597
	Finding offline computers	598
	Finding unscanned computers	598
	Viewing risks	599
	Running a report on the deployment status of clients	600
	Viewing attack targets and sources	601
	Generating a list of the Symantec Endpoint Protection versions installed on the clients and servers in your network	602
	Configuring reporting preferences	602
	Logging on to reporting from a stand-alone Web browser	603
	About the types of reports	604
	Running and customizing quick reports	606
	Saving and deleting custom reports	608
	How to generate scheduled reports	609
	Editing the filter used for a scheduled report	611
	Printing and saving a copy of a report	612
	Viewing logs	613
	What you can do from the logs	614
	Saving and deleting custom logs by using filters	617
	Viewing logs from other sites	618
Chapter 26	Managing notifications	620
	Managing notifications	620
	How notifications work	621
	What are the types of notifications and when are they sent?	622
	About partner notifications	627
	Establishing communication between the management server and email servers	628
	Viewing and acknowledging notifications	628

	Saving and deleting administrative notification filters	630
	Setting up administrator notifications	630
	How upgrades from another version affect notification conditions	632
Section 7	Protecting clients in virtual environments	634
Chapter 27	Overview of Symantec Endpoint Protection and virtual infrastructures	635
	Using Symantec Endpoint Protection in virtual infrastructures	635
	About Shared Insight Cache	637
	About the Virtual Image Exception tool	638
Chapter 28	Installing and using a network-based Shared Insight Cache	639
	What do I need to do to use a network-based Shared Insight Cache?	639
	System requirements for implementing a network-based Shared Insight Cache	640
	Installing and uninstalling a network-based Shared Insight Cache	641
	Enabling or disabling the use of a network-based Shared Insight Cache	643
	Customizing network-based Shared Insight Cache configuration settings	644
	About stopping and starting the network-based Shared Insight Cache service	648
	Viewing network-based Shared Insight Cache log events	648
	Monitoring network-based Shared Insight Cache performance counters	650
	Troubleshooting issues with Shared Insight Cache	651
Chapter 29	Installing a Security Virtual Appliance and using a vShield-enabled Shared Insight Cache	652
	What do I need to do to use a vShield-enabled Shared Insight Cache?	653
	What do I need to do to install a Security Virtual Appliance?	654
	About the Symantec Endpoint Protection Security Virtual Appliance	655
	VMware software requirements to install a Symantec Security Virtual Appliance	657

	VMware software requirements for the Guest Virtual Machines	658
	Configuring the Symantec Endpoint Protection Security Virtual Appliance installation settings file	658
	Installing a Symantec Endpoint Protection Security Virtual Appliance	662
	Enabling Symantec Endpoint Protection clients to use a vShield-enabled Shared Insight Cache	665
	Stopping and starting the vShield-enabled Shared Insight service	665
	Service commands for the vShield-enabled Shared Insight Cache	666
	Configuration file settings for a vShield-enabled Shared Insight Cache	666
	About vShield-enabled Shared Insight Cache event logging	669
	Uninstalling a Symantec Endpoint Protection Security Virtual Appliance	670
Chapter 30	Using Virtual Image Exception	671
	Using the Virtual Image Exception tool on a base image	671
	System requirements for the Virtual Image Exception tool	672
	Running the Virtual Image Exception tool	673
	Configuring Symantec Endpoint Protection to bypass the scanning of base image files	673
Chapter 31	Non-persistent virtual desktop infrastructures	675
	Using Symantec Endpoint Protection in non-persistent virtual desktop infrastructures	675
	Setting up the base image for non-persistent guest virtual machines in VDIs	676
	Creating a registry key to mark the base image Guest Virtual Machines (GVMs) as non-persistent clients	677
	Configuring a separate purge interval for offline non-persistent VDI clients	678

Section 8	Configuring and managing the management server	679
Chapter 32	Configuring the connection between the management server and the clients	680
	Setting up SSL communications between a Symantec Endpoint Protection Manager and the clients	680
	Verifying port availability	681
	Changing the Apache SSL port assignment for client communication	682
	Enabling SSL for the Apache web server for client communication	683
	Improving client and server performance	685
	About server certificates	687
	Best practices for updating server certificates and maintaining the client-server connection	688
	Disabling or enabling secure communications between the server and the client	689
	Updating or restoring a server certificate	690
Chapter 33	Configuring the management server	692
	Managing Symantec Endpoint Protection Manager servers and third-party servers	692
	About the types of Symantec Endpoint Protection servers	695
	Exporting and importing server settings	695
	Enabling or disabling Symantec Endpoint Protection Manager web services	696
Chapter 34	Managing databases	698
	Maintaining the database	698
	Scheduling automatic database backups	702
	Scheduling automatic database maintenance tasks	703
	Increasing the Microsoft SQL Server database file size	704
	Exporting data to a Syslog server	705
	Exporting log data to a text file	706
	Exporting log data to a comma-delimited text file	707
	Specifying client log size and which logs to upload to the management server	708
	Specifying how long to keep log entries in the database	709
	About increasing the disk space on the server for client log data	709

	Clearing log data from the database manually	710
Chapter 35	Managing failover and load balancing	712
	Setting up failover and load balancing	712
	About failover and load balancing	713
	Configuring a management server list for load balancing	715
	Assigning a management server list to a group and location	716
Chapter 36	Managing sites and replication	718
	Setting up sites and replication	718
	Deciding whether or not to set up multiple sites and replication	720
	About determining how many sites you need	722
	How replication works	724
	How to resolve data conflicts between sites during replication	726
	Replicating data without a schedule	727
	Replicating data on a schedule	728
	Specifying which data to replicate	729
	Deleting replication partners	729
	Re-adding a replication partner that you previously deleted	730
Chapter 37	Preparing for disaster recovery	732
	Preparing for disaster recovery	732
	Backing up the database and logs	733
	Backing up a server certificate	735
Section 9	Troubleshooting Symantec Endpoint Protection Manager	736
Chapter 38	Performing disaster recovery	737
	Performing disaster recovery	737
	Reinstalling or reconfiguring Symantec Endpoint Protection Manager	738
	Generating a new server certificate	740
	Restoring the database	740

Chapter 39	Troubleshooting installation and communication problems	742
	Troubleshooting Symantec Endpoint Protection	742
	Troubleshooting computer issues with the Symantec Help support tool	744
	Identifying the point of failure of an installation	744
	Troubleshooting communication problems between the management server and the client	745
	Checking the connection to the management server on the client computer	747
	Investigating protection problems using the troubleshooting file on the client	748
	Enabling and viewing the Access log to check whether the client connects to the management server	748
	Stopping and starting the Apache Web server	749
	Using the ping command to test the connectivity to the management server	750
	Using a browser to test the connectivity to Symantec Endpoint Protection Manager on the Symantec Endpoint Protection client	750
	Checking the debug log on the client computer	751
	Checking the inbox logs on the management server	751
	Restoring client-server communication settings by using the SylinkDrop tool	752
	Troubleshooting communication problems between the management server and the console or the database	754
	Verifying the connection with the database	755
	Client and server communication files	757
Chapter 40	Troubleshooting reporting issues	758
	Troubleshooting reporting issues	758
	Changing timeout parameters for reviewing reports and logs	759
	Accessing reporting pages when the use of loopback addresses is disabled	762
Chapter 41	Using Power Eraser to troubleshoot difficult and persistent threats	763
	What you should know before you run Power Eraser from the Symantec Endpoint Protection Manager console	763
	Tasks to perform when you need to run Power Eraser from the Symantec Endpoint Protection Manager console	766

	Starting Power Eraser analysis from Symantec Endpoint Protection Manager	770
	Responding to Power Eraser detections	772
Appendix A	Client feature comparison tables	775
	Client protection features based on platform	775
	Management features based on platform	776
	Virus and Spyware Protection policy settings based on platform	781
	Intrusion Prevention policy settings based on platform	784
	LiveUpdate policy settings based on platform	785
	Exceptions policy settings based on platform	786
Appendix B	Customizing and deploying the Windows client installation by using third-party tools	788
	Installing Windows client software using third-party tools	789
	About client installation features and properties	790
	About configuring MSI command strings	791
	About configuring Setaid.ini	791
	Symantec Endpoint Protection command-line client installation properties	792
	Symantec Endpoint Protection command-line client features	793
	Windows Installer parameters	794
	Windows Security Center properties	796
	Command-line examples for installing the Windows client	798
	Installing Windows clients with Microsoft SCCM/SMS	798
	Installing Windows clients with an Active Directory Group Policy Object (GPO)	799
	Creating a GPO software distribution	801
	Adding computers to an organizational unit to install software	803
	Copying a Sylink.xml file to make a managed installation package	803
	Uninstalling client software with an Active Directory Group Policy Object	804
Appendix C	Command-line options for the Windows client	806
	Running the Windows client using the <code>smc</code> command-line interface	806
	<code>smc</code> command error codes	810

Appendix D	Command-line options for the Virtual Image	
	Exception tool	812
	vietool	813
Appendix E	Syntax for custom intrusion prevention signatures	
	and application control rules	815
	Regular expressions in Symantec Endpoint Protection Manager	816
	About signature syntax and conventions	818
	Protocol type arguments	819
	TCP protocol arguments	819
	UDP protocol arguments	821
	ICMP protocol arguments	822
	IP protocol arguments	823
	Msg arguments	826
	Content arguments	827
	Optional content arguments	827
	Case-sensitivity	828
	HTTP decoding	828
	Offset and depth	828
	Streamdepth arguments	829
	Supported operators	830
	Sample custom IPS signature syntax	830
Index		833

Introducing Symantec Endpoint Protection

This chapter includes the following topics:

- [What is Symantec Endpoint Protection?](#)
- [What's new in Symantec Endpoint Protection 12.1.6](#)
- [How Symantec Endpoint Protection uses layers to protect computers](#)
- [How does Symantec Endpoint Protection enforce compliance?](#)

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.

Symantec Endpoint Protection protects your network by accomplishing the following key tasks:

- Protects your endpoints from malware and maximizes system uptime.

See [“How Symantec Endpoint Protection uses layers to protect computers”](#) on page 36.

- Enforces protection policies and compliance on the endpoint.
See [“How does Symantec Endpoint Protection enforce compliance?”](#) on page 38.
- Responds to threats and incidents effectively by quickly quarantining and removing malware from endpoints.
See [“Managing the Quarantine”](#) on page 445.
- Monitors and tracks risk exposure across platforms, devices, remote locations, and in physical, virtual or hybrid environments.
See [“Monitoring endpoint protection”](#) on page 593.

See [“Components of Symantec Endpoint Protection”](#) on page 50.

What's new in Symantec Endpoint Protection 12.1.6

This version of Symantec Endpoint Protection includes new features in the following areas:

- [System requirements](#)
- [Installation files](#)
- [Windows Embedded platform support](#)
- [Protection features](#)
- [Reporting](#)
- [Removed or unsupported features](#)
- [Documentation](#)

System requirements

Symantec Endpoint Protection includes the following additional support:

Operating system support:

- Red Hat Enterprise Linux (RHEL) 7.0 and 7.1
- Oracle Linux (OEL) 6U5

Browser support:

- Microsoft Internet Explorer 11
- Mozilla Firefox 5.x through 38.0.1
- Google Chrome through 42.0.2311.152

Installation files

You can now download a full installation file from FileConnect. This single installation file includes Symantec Endpoint Protection Manager, the Windows, Mac, and Linux clients, the supplemental tools, and some of the virtualization tools:

Symantec_Endpoint_Protection_12.1.6_Full_Installation_*language*.exe

If you download the full installation file, you do not need the following individual files:

- For the standalone client installers for Windows, Mac, and Linux, download:
Symantec_Endpoint_Protection_12.1.6_All_Clients_*language*.zip
- For the management console and management server, download:
Symantec_Endpoint_Protection_12.1.6_SEPM_*language*.zip
- For the virtualization tools, such as Security Virtual Appliance or Shared Insight Cache, download:
Symantec_Endpoint_Protection_12.1.5_Virtual_Toolkit_ML.zip

For information on all of the installation files, see:

[A guide to Endpoint Protection files on FileConnect](#)

You access FileConnect from the following URL:

<https://fileconnect.symantec.com>

Windows Embedded platform support

- Symantec Endpoint Protection includes the following additional support for the clients that run on Windows Embedded devices and in virtual desktop infrastructure (VDI) environments.
 - A reduced-size client installation package
The Client Deployment wizard includes a reduced-size client installation package for computers with a smaller footprint, such as Windows Embedded devices and virtual environments. The client installation package also determines if the Windows Embedded operating system has the appropriate components installed. If the device does not, a message appears where you can click a link to more information on which components you need.
See [“About reduced-size client installation packages”](#) on page 114.
See [“Installing clients with Save Package”](#) on page 122.
 - Reduced-size definitions for Windows clients
You can install a smaller set of virus and spyware definitions, which are 80 percent to 90 percent smaller than the standard-size definitions. After you install the client, you continue to update the older reduced-size definitions with newer reduced-size definitions. For each site, you download the

definitions to the management server. You can download reduced-size definitions only, standard-size definitions only, or both at the same time.

See [“Configuring a site to download content updates”](#) on page 189.

See [“Configuring the types of content used to update client computers”](#) on page 196.

The reduced-size content provides slightly less Virus and Spyware Protection than the standard-size content. Symantec recommends that you install and enable all protection technologies to mitigate this small reduction in Virus and Spyware Protection. These protection technologies include the firewall, Download Insight, intrusion prevention, and SONAR. Symantec also recommends that you use system lockdown to ensure the highest level of security.

See [“Configuring system lockdown”](#) on page 541.

See [“Automatically updating whitelists or blacklists for system lockdown”](#) on page 554.

- **Support for Windows Embedded write filters**
 Windows Embedded operating systems use write filters to redirect the changes to an overlay so that changes won't persist after the device is restarted. During installation, the Symantec Endpoint Protection installer detects if write filters are installed or enabled. Symantec Endpoint Protection then notifies you if you need to change a writer filter status to the disabled status to continue the installation. To ensure that the client installation, the virus definitions, and the product running state persist after each restart, Symantec Endpoint Protection adds exclusions to write filters for its file paths and registry keys.
 Symantec Endpoint Protection supports the File-Based Write Filter (FBWF) for Windows XP Embedded, Windows 7 Embedded, and Windows 8 Embedded. Symantec Endpoint Protection does not support the Unified Write Filter (UWF) or the Enhanced Write Filter (EWF).
 See [“About reduced-size client installation packages”](#) on page 114.
- **Ability to search for information about Windows Embedded devices**
 You can search for clients based on their installation type or write filter state. For example, you can find out which clients have the latest reduced-size definitions. To search, click **Clients > Clients > Search clients**. In the **Search Field**, select **Install type** for definitions or **Enhanced Write Filter, File Based File Filter, Unified File Filter** for the write filter type.
 See [“Searching for information about client computers”](#) on page 255.
- **Reports on Windows Embedded devices**
 You can run reports or view logs on the devices that run the Windows Embedded operating system. You can search on either all versions or specific versions of the operating system. To view logs based on the operating

system, in the console, click **Monitors > Logs > Computer Status > Advanced Settings > Operating system**.

See [“How to generate scheduled reports”](#) on page 609.

See [“Viewing logs”](#) on page 613.

Protection features

- Integration with Symantec Advanced Threat Protection: Endpoint (ATP: Endpoint)
ATP: Endpoint is an on-premises virtual appliance that detects advanced threats on endpoints in your network. ATP: Endpoint delivers actionable data so that you can quickly analyze and respond to the threats. You can select threats to block and add them to the ATP: Endpoint policy. When ATP: Endpoint sends the policy to the Symantec Endpoint Protection Manager, read-only file fingerprints from ATP: Endpoint appear in the system lockdown configuration. You can also configure Symantec Endpoint Protection Manager client groups to use ATP: Endpoint for reputation queries and submissions.
See [“Configuring client groups to use private servers for reputation queries and submissions”](#) on page 457.
- System lockdown enhancements
Collect file fingerprint lists for system lockdown for a group of clients
You can run a new command from the management console to collect file fingerprints for all the applications that a group of client computers run. The best time to use this method is to add file fingerprints to whitelists. Another common use of this command is to create a list of whitelisted applications for a master image for a Windows Embedded device. In the console, click **Clients**, right-click a group, and click **Run a command on the group > Collect File Fingerprint List**.
The blacklist mode is automatically enabled in 12.1.6. You do not have to edit the `conf.properties` file to enable it.
See [“Configuring system lockdown”](#) on page 541.
See [“Running commands on client computers from the console”](#) on page 261.
- Bandwidth usage reduction when virus and spyware definitions are downloaded to clients
When too many clients simultaneously request full definition downloads from the management server, Symantec Endpoint Protection helps to prevent network overloads. If the management server downloads full definitions only rather than deltas, you can specify that clients get deltas from a LiveUpdate server instead. You can also block clients from downloading full definitions from the management server. You can also receive an alert if too many clients request full downloads from the management server.
See [“Mitigating network overloads for client update requests”](#) on page 193.

- **Aggressive scan mode**
If Windows client detects a large number of viruses, spyware, or high-risk threats, an aggressive scan mode engages automatically. The scan restarts and uses Insight lookups. You can pause or cancel the scan when it is in aggressive mode. However, you cannot configure the aggressive scan mode in either the Virus and Spyware Protection policy or the client.
- **Auto-compile for Symantec Endpoint Protection client for Linux**
The Symantec Endpoint Protection client installer for Linux can now auto-compile the Auto-Protect kernel module. The installer takes this action when the operating system kernel is not compatible with the precompiled Auto-Protect kernel modules.

Reporting

- **Content Distribution Monitor tool**
The Content Distribution Monitor tool helps you manage and monitor multiple Group Update Providers (GUPs) in your environment. The tool displays a graphical display of the GUPs' health and content distribution status. The Content Distribution Monitor tool was provided but was unsupported with previous versions. The tool is now supported and included in the Tools/ContentDistributionMonitor folder of the installation file.

Removed or unsupported features

- Symantec Endpoint Protection 12.1.6 no longer supports an installation on Windows XP Service Pack 2 (32-bit).
- Symantec Endpoint Protection 12.1.6 is the last release to support the installation of Symantec Endpoint Protection Manager on any version of Windows XP/Windows Server 2003, or to any 32-bit operating system. This upcoming change does not affect the Symantec Endpoint Protection client.
- 12.1.5 was the last release to add new features for Symantec Network Access Control. Version 12.1.6 does not have a separate installation file for Symantec Network Access Control. For 12.1.6, you enable the Symantec Network Access Control functionality by using the `snac.xml` file that is located in the `SNAC_12.1.6_XML_Multi.zip` file on FileConnect. The Symantec Endpoint Protection Manager Help still includes information on the Symantec Network Access Control features.
See [“Enabling Symantec Network Access Control functionality in Symantec Endpoint Protection”](#) on page 161.
- Symantec Endpoint Protection 12.1.6 does not ship with Small Business Edition, which reached end of life (EOL) in May, 2015. Small Business Edition 12.1 customers can use a tool to migrate to the cloud-based Symantec Endpoint Protection Small Business Edition. For more information, see:

[Migrating to Symantec Endpoint Protection Small Business Edition](#)

See [“Supported upgrade paths to Symantec Endpoint Protection”](#) on page 148.

- Symantec Endpoint Protection for Windows XP Embedded 5.1 reaches end of life (EOL) in June, 2015. Symantec Endpoint Protection Windows XP Embedded 5.1 customers can migrate to Symantec Endpoint Protection 12.1.6, but must first uninstall Symantec Endpoint Protection Windows XP Embedded 5.1.
[Migrating from Symantec Endpoint Protection for Windows XP Embedded 5.1 to Endpoint Protection \(SEP\) 12.1.6](#)
- Symantec Endpoint Protection Manager no longer supports LiveUpdate Administration Utility 1.x, which reached end of life on January 5, 2015. Also, the LiveUpdate Settings policy no longer includes the option to enable support for LiveUpdate Administration Utility 1.x. If you use this utility in your environment, you should migrate to LiveUpdate Administrator 2.3.x. To get the latest version of LiveUpdate Administrator, see:
[Downloading LiveUpdate Administrator](#)
 See [“Setting up an internal LiveUpdate server for Symantec Endpoint Protection clients”](#) on page 211.
- Symantec Endpoint Protection 12.1.6 no longer supports Symantec Protection Center version 2.0.
- Symantec Endpoint Protection no longer ships with the free Symantec Endpoint Protection Integration Component. The Integration Component combines Symantec Endpoint Protection with other Symantec Management Platform solutions. The Integration Component was in the Tools\SEPIntegrationComponent folder of the installation file.

Documentation

- Symantec Endpoint Protection includes a new Quick Start guide. This guide provides a step-by-step walk-through for installing 100 or fewer managed clients.
[Symantec Endpoint Protection Quick Start Guide](#)
- Symantec Endpoint Protection includes new documentation for the following tools, which are located in the Tools folder of the installation file:
 - Apache Reverse Proxy
 - CleanWipe
 - Content Distribution Monitor
 - Push Deployment Wizard
 - SylinkDrop
 - SymHelp

How Symantec Endpoint Protection uses layers to protect computers

Symantec's core protection against known and unknown threats uses a layered approach to defense. The layered 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.

[Table 1-1](#) describes the types of protection that Symantec Endpoint Protection Manager uses to protect your network.

Table 1-1 The layers of protection that are integrated into Symantec Endpoint Protection

Layer	Type of protection	Description	Symantec Endpoint Protection technology name
1	Network-based protection	<p>The firewall and the intrusion prevention system block over 60% of malware as it travels over the network and before it arrives at the computer.</p> <p>This primary defense protects against drive-by downloads, social engineering, fake antivirus programs, individual system vulnerabilities, rootkits, botnets, and more. Stopping malware before it reaches your computer is definitely preferred to identifying a vulnerability that has already been exploited.</p>	<p>Network Threat Protection:</p> <ul style="list-style-type: none"> ■ Firewall ■ Protocol-aware IPS <p>Virus and Spyware Protection:</p> <ul style="list-style-type: none"> ■ Browser protection <p>See “Managing firewall protection” on page 336.</p> <p>See “Managing intrusion prevention on client computers” on page 380.</p> <p>See “Modifying miscellaneous settings for Virus and Spyware Protection on Windows computers” on page 475.</p>
2	File-based protection	<p>This traditional signature-based antivirus protection looks for and eradicates the malware that has already taken up residence on a system. Virus and Spyware Protection blocks and removes the malware that arrives on the computer by using scans.</p> <p>Unfortunately, many companies leave themselves exposed through the belief that antivirus alone keeps their systems protected.</p>	<p>Virus and Spyware Protection:</p> <ul style="list-style-type: none"> ■ Antivirus engine ■ Auto-Protect ■ Bloodhound <p>See “Managing scans on client computers” on page 405.</p>

Table 1-1 The layers of protection that are integrated into Symantec Endpoint Protection (*continued*)

Layer	Type of protection	Description	Symantec Endpoint Protection technology name
3	Reputation-based protection	<p>Insight establishes information about entities, such as websites, files, and IP addresses to be used in effective security.</p> <p>Download Insight determines the safety of files and websites by using the wisdom of the community. Sophisticated threats require leveraging the collective wisdom of over 200 million systems to identify new and mutating malware. Symantec's Insight gives companies access to the largest global intelligence network available to allow them to filter every file on the internet based on reputation.</p>	<p>Virus and Spyware Protection:</p> <ul style="list-style-type: none"> ■ Domain reputation score ■ File reputation (Insight) <p>See “Managing Download Insight detections” on page 432.</p>
4	Behavioral-based protection	<p>SONAR looks at processes as they execute and use malicious behaviors to indicate the presence of malware.</p> <p>SONAR watches programs as they run, and blocks suspicious behaviors. SONAR catches targeted and unknown threats by aggressively monitoring file processes as they execute and identify malicious behavior. SONAR uses artificial intelligence, behavior signatures, and policy lockdown to monitor nearly 1,400 file behaviors as they execute in real time. When SONAR is combined with Insight, this technology is able to aggressively stop zero-day threats without increasing false-positives.</p>	<ul style="list-style-type: none"> ■ Proactive Threat Protection (Virus and Spyware Protection policy): SONAR <p>See “Managing SONAR” on page 486.</p>
5	Repair and remediation tools	<p>When malware does get through, Power Eraser scrubs hard-to-remove infections and gets your system back online as quickly as possible. Power Eraser uses aggressive remediation on hard-to-remove infections.</p>	<p>Power Eraser:</p> <ul style="list-style-type: none"> ■ Boot to clean operating system ■ Power Eraser uses aggressive heuristics ■ Threat-specific tools <p>See “What you should know before you run Power Eraser from the Symantec Endpoint Protection Manager console” on page 763.</p>

Symantec Endpoint Protection extends and enhances security with the following additional technologies:

- **System Lockdown**
System Lockdown lets you limit the applications that can run. System Lockdown operates in either a whitelisting or a blacklisting mode. 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 541.
- **Application control**
Application control monitors and controls an application's behavior. Application control protects against unauthorized access and attack by controlling what applications can run. Application control blocks or terminates processes, limits file and folder access, protects the Windows registry, and controls module and DLL loading. Application control includes predefined templates that block application behaviors known to be malicious.
See [“About application and device control”](#) on page 523.
See [“Setting up application and device control”](#) on page 526.
- **Device control**
Device control restricts and enables the access to the hardware that can be used on the client computer. You can block and control the devices that are connected to your systems, such as USB devices, FireWire, serial, and parallel ports. Device control can prevent all access to a port or allow access only from certain devices with a specific vendor ID.
See [“Configuring device control”](#) on page 569.

See [“How does Symantec Endpoint Protection enforce compliance?”](#) on page 38.

How does Symantec Endpoint Protection enforce compliance?

Symantec Endpoint Protection also ensures that the client computers meet compliance requirements. You may need to enforce the company's security policy, such as blocking computers from opening certain applications or websites. Or, you may need to prevent security breaches and enforce security and privacy-related regulations. For example, Symantec solutions help healthcare organizations to enforce healthcare data provisions against medical identity theft.

Symantec Endpoint Protection uses the following tools to enforce compliance requirements:

- **Host Integrity**

The Host Integrity policy ensures that the endpoints are protected and compliant. For example, you can make sure that every computer is running a firewall or a particular operating system security patch.

See [“How Host Integrity works”](#) on page 571.

- Reporting and analytics

Symantec Endpoint Protection provides multi-dimensional analysis, robust graphical reporting, and an easy-to-use Dashboard. You can use reports and logs to check that the computers in your network are connected, protected, and compliant with company policy.

See [“Monitoring endpoint protection”](#) on page 593.

See [“How Symantec Endpoint Protection uses layers to protect computers”](#) on page 36.

Installing Symantec Endpoint Protection

- [Chapter 2. Planning the installation](#)
- [Chapter 3. Installing Symantec Endpoint Protection Manager](#)
- [Chapter 4. Managing product licenses](#)
- [Chapter 5. Installing the Symantec Endpoint Protection client](#)
- [Chapter 6. Upgrading Symantec Endpoint Protection](#)

Planning the installation

This chapter includes the following topics:

- [Getting up and running on Symantec Endpoint Protection for the first time](#)
- [Components of Symantec Endpoint Protection](#)
- [Optional components for Symantec Endpoint Protection](#)
- [System requirements for Symantec Endpoint Protection](#)
- [Product license requirements](#)
- [Supported virtual installations and virtualization products](#)
- [Network architecture considerations](#)
- [About choosing a database type](#)
- [About basic management server settings](#)
- [Management server ports](#)
- [About SQL Server configuration settings](#)
- [About SQL Server database authentication modes](#)

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

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

[Table 2-1](#) lists the tasks that you should perform to install and protect the computers in your network immediately.

Table 2-1 Tasks to install and configure Symantec Endpoint Protection

Step	Action	Description
1	Plan your installation structure	<p>Before you install the product, consider the size and geographical distribution of your network to determine the installation architecture.</p> <p>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.</p> <ul style="list-style-type: none"> ■ 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. <p>To help you plan medium to large-scale installations, see: Symantec Endpoint Protection Sizing and Scalability Best Practices White Paper.</p> <p>See “Network architecture considerations” on page 64.</p> <p>See “Setting up sites and replication” on page 718.</p> <p>See “Setting up failover and load balancing” on page 712.</p>

Table 2-1 Tasks to install and configure Symantec Endpoint Protection
(continued)

Step	Action	Description
2	Prepare for and then install Symantec Endpoint Protection Manager	<p>1 Make sure the computer on which you install the management server meets the minimum system requirements.</p> <p>See: Release Notes and System Requirements for all versions of Symantec Endpoint Protection and Symantec Network Access Control</p> <p>2 To install Symantec Endpoint Protection Manager, you must be logged on with an account that grants local administrator access.</p> <p>3 Decide on whether to install the embedded database or use a Microsoft SQL Server database.</p> <p>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.</p> <p>See “About SQL Server configuration settings” on page 68.</p> <p>See “Setting up failover and load balancing” on page 712.</p> <p>4 You install Symantec Endpoint Protection Manager first. After you install, you immediately configure the installation with the Management Server Configuration Wizard.</p> <p>Decide on the following items when you configure the management server:</p> <ul style="list-style-type: none"> ■ A password for your login to the management console ■ An email address where you can receive important notifications and reports ■ An encryption password, which may be needed depending on the options that you select during installation <p>See “Installing Symantec Endpoint Protection Manager” on page 74.</p> <p>See “About basic management server settings” on page 65.</p> <p>See “Configuring Symantec Endpoint Protection Manager during installation” on page 76.</p>

Table 2-1 Tasks to install and configure Symantec Endpoint Protection
(continued)

Step	Action	Description
3	Add groups, policies, and locations	<p>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.</p> <p>If you add new groups, you can use the following group structure as a basis:</p> <ul style="list-style-type: none"> ■ Desktops ■ Laptops ■ Servers <p>See “Importing existing groups and computers from an Active Directory or an LDAP server” on page 240.</p> <p>See “How you can structure groups” on page 238.</p> <p>See “Adding a group” on page 239.</p> <p>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.</p> <p>You can set up a location that allows the mobile computers that are not in the office to update their definitions automatically from Symantec's LiveUpdate servers.</p> <p>See Best Practices for Symantec Endpoint Protection Location Awareness.</p> <p>See “Adding a location to a group” on page 279.</p> <p>3 Disable inheritance for the groups or locations for which you want to use different policies or settings.</p> <p>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.</p> <p>See “Disabling and enabling a group's inheritance” on page 247.</p> <p>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.</p>

Table 2-1 Tasks to install and configure Symantec Endpoint Protection
(continued)

Step	Action	Description
4	Change communication settings to increase performance	<p>You can improve network performance by modifying the following client-server communication settings in each group:</p> <ul style="list-style-type: none"> ■ 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. <p>See “Randomizing content downloads from the default management server or a Group Update Provider” on page 207.</p> <p>See “Configuring push mode or pull mode to update client policies and content” on page 170.</p>
5	Activate the product license	<p>Purchase and activate a license within 60 days of product installation.</p> <p>See “Licensing Symantec Endpoint Protection” on page 92.</p> <p>See “Product license requirements” on page 61.</p> <p>See “Activating or importing your Symantec Endpoint Protection 12.1.x product license” on page 96.</p>

Table 2-1 Tasks to install and configure Symantec Endpoint Protection
(continued)

Step	Action	Description
6	Decide on a client deployment method	<p>Determine which client deployment method would work best to install the client software on your computers in your environment.</p> <p>See “About client installation methods” on page 115.</p> <ul style="list-style-type: none"> ■ 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: <ul style="list-style-type: none"> ■ 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 “About the communication ports that Symantec Endpoint Protection uses” on page 113. ■ 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 111. <p>See “Preparing for client installation” on page 108.</p>

Table 2-1 Tasks to install and configure Symantec Endpoint Protection
(continued)

Step	Action	Description
7	Prepare the client for installation	<p>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.</p> <p>See: Release Notes and System Requirements for all versions of Symantec Endpoint Protection and Symantec Network Access Control</p> <p>2 Manually uninstall any third-party security software programs from Windows computers that the Symantec Endpoint Protection client installer cannot uninstall.</p> <p>For a list of products that this feature removes, see: Third-party security software removal support in Symantec Endpoint Protection</p> <p>See “Configuring client packages to uninstall existing third-party security software” on page 127.</p> <p>You must uninstall any existing security software from Linux computers or from Mac computers.</p> <p>Some programs may also have special uninstallation routines. See the documentation for the third-party software.</p>

Table 2-1 Tasks to install and configure Symantec Endpoint Protection
(continued)

Step	Action	Description
8	Deploy to install the client software	<p>1 For Windows clients, do the following tasks:</p> <ul style="list-style-type: none"> ■ Create a custom client install feature set to determine which components you install on the client computers. You can also use one of the default client install feature sets. <p>Make sure that you keep computer mode and not user mode. Most Symantec Endpoint Protection users use computer mode. 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.</p> <p>See “Switching a Windows client between user mode and computer mode” on page 263.</p> <p>See “Importing existing groups and computers from an Active Directory or an LDAP server” on page 240.</p> <p>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.</p> <ul style="list-style-type: none"> ■ 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. <p>See “Configuring Windows client installation feature sets” on page 127.</p> <p>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.</p> <p>See “Installing clients with Web Link and Email” on page 118.</p> <p>See “Installing clients with Remote Push” on page 120.</p> <p>See “Installing clients with Save Package” on page 122.</p> <p>See “Exporting client installation packages” on page 124.</p> <p>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.</p>

Table 2-1 Tasks to install and configure Symantec Endpoint Protection
(continued)

Step	Action	Description
9	Check that the computers are listed in the groups that you expected and that the clients communicate with the management server	<p>In the management console, on the Clients > Clients page:</p> <ol style="list-style-type: none"> 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: <ul style="list-style-type: none"> ■ The Name column displays a green dot for the clients that are connected to the management server. See “How to determine whether the client is connected in the console” on page 167. ■ The Last Time Status Changed column displays the time that each client last communicated with the management server. ■ The Restart Required column displays the client computers you need to restart to enable protection. See “Restarting the client computers from Symantec Endpoint Protection Manager” on page 129. ■ 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 172. See “Manually updating policies on the client” on page 315. 2 Change to the Protection technology view and ensure that the status is set to On in the columns between and including AntiVirus Status and Tamper Protection Status. See “Viewing the protection status of clients and client computers” on page 253. 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 747. <p>See “How to determine whether the client computer is connected and protected” on page 169.</p> <p>See “Troubleshooting communication problems between the management server and the client” on page 745.</p>

See [“What do I do after I install the management server?”](#) on page 88.

See [“What you can do from the console”](#) on page 86.

Components of Symantec Endpoint Protection

[Table 2-2](#) describes the main components of Symantec Endpoint Protection.

Table 2-2 Main product components

Component	Description
Symantec Endpoint Protection Manager	<p>Symantec Endpoint Protection Manager is a management server that manages the client computers that connect to your company's network.</p> <p>Symantec Endpoint Protection Manager includes the following subcomponents:</p> <ul style="list-style-type: none"> ■ 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. <p>See “What you can do from the console” on page 86.</p> <p>See “Installing Symantec Endpoint Protection Manager” on page 74.</p>
Symantec Endpoint Protection client	<p>The Symantec Endpoint Protection client runs on the following platforms:</p> <ul style="list-style-type: none"> ■ The Windows client protects computers by using virus and spyware scans, SONAR, Download Insight, a firewall, an intrusion prevention system, and other protection technologies. It runs on the servers, desktops, and portable computers that you want to protect. ■ The Symantec Endpoint Protection Mac client protects computers by using virus and spyware scans and an intrusion prevention system. ■ The Symantec Endpoint Protection Linux client protects computers by using virus and spyware scans. <p>See “What is Symantec Endpoint Protection?” on page 29.</p>

See [“Optional components for Symantec Endpoint Protection”](#) on page 51.

See [“How Symantec Endpoint Protection uses layers to protect computers”](#) on page 36.

Optional components for Symantec Endpoint Protection

Table 2-3 lists the additional components that you can download and use with Symantec Endpoint Protection.

Table 2-3 Optional components and their function

Component	Description
LiveUpdate Administrator	<p>LiveUpdate Administrator downloads definitions, signatures, and product updates 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.</p> <p>The LiveUpdate Administrator is located in the LiveUpdate folder in the Tools installation file.</p> <p>See “Choose a distribution method to update content on clients” on page 182.</p> <p>See “Setting up an internal LiveUpdate server for Symantec Endpoint Protection clients” on page 211.</p>
Group Update Provider (GUP)	<p>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.</p> <p>See “Using Group Update Providers to distribute content to clients” on page 215.</p>
Central Quarantine	<p>The Central Quarantine receives suspicious files and unrepaired infected items from the Symantec Endpoint Protection clients. The Central Quarantine forwards a sample to Symantec Security Response, which analyzes the sample. If a threat is new, Symantec Security Response produces security updates.</p> <p>The Central Quarantine is located in the Tools\CentralQ folder.</p> <p>For more information, see the <i>Symantec Central Quarantine Implementation Guide</i>.</p> <p>See “Configuring clients to submit quarantined items to a Central Quarantine Server or Symantec Security Response” on page 448.</p>

Table 2-3 Optional components and their function (*continued*)

Component	Description
Shared Insight Cache and Security Virtual Appliance	<p>These components enhance the scanning on virtual environments.</p> <p>The Symantec Endpoint Protection Security Virtual Appliance is a Linux-based virtual appliance that you install on a VMware ESX/ESXi server. The Security Virtual Appliance integrates with VMware's vShield Endpoint. The Shared Insight Cache runs in the appliance and lets Windows-based Guest Virtual Machines (GVMs) with the Symantec Endpoint Protection client installed share scan results.</p> <p>The virtualization tools are located in the Tools\Virtualization folder.</p> <p>See "About the Symantec Endpoint Protection Security Virtual Appliance" on page 655.</p>
IT Analytics server	<p>The IT Analytics tool expands upon the built-in reports in Symantec Endpoint Protection Manager by enabling you to create custom reports and custom queries. The tool also offloads the reporting burden from the management server to another server. IT Analytics keeps information for a longer period of time, enforces compliance, reduces costs, and provides summaries.</p> <p>The IT Analytics tool and documentation is located in the Tools\ITAnalytics folder.</p>

See ["Components of Symantec Endpoint Protection"](#) on page 50.

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.

- See ["System requirements for Symantec Endpoint Protection Manager"](#) on page 53.
- See ["System requirements for the Symantec Endpoint Protection client for Windows"](#) on page 55.
- See ["System requirements for the Symantec Endpoint Protection client for Windows Embedded"](#) on page 56.
- See ["System requirements for the Symantec Endpoint Protection client for Mac"](#) on page 57.
- See ["System requirements for the Symantec Endpoint Protection client for Linux"](#) on page 58.

See ["Getting up and running on Symantec Endpoint Protection for the first time"](#) on page 41.

See [“Supported virtual installations and virtualization products”](#) on page 62.

See [“Internationalization requirements”](#) on page 59.

System requirements for Symantec Endpoint Protection Manager

Table 2-4 Symantec Endpoint Protection Manager system requirements

Component	Requirements
Processor	<ul style="list-style-type: none"> ■ 32-bit processor: Intel Pentium 4 or equivalent (minimum dual core or hyper-threading recommended) ■ 64-bit processor: Intel Pentium 4 with x86-64 support or equivalent (minimum dual core or hyper-threading recommended) <p>Note: Intel Itanium IA-64 processors are not supported.</p>
Physical RAM	<p>2 GB RAM available minimum; 4 GB or more available recommended.</p> <p>Note: Your Symantec Endpoint Protection Manager server may require additional RAM depending on the RAM requirements of other applications that are already installed.</p>
Hard drive	<p>16 GB available minimum (100 GB recommended) for the management server.</p> <p>40 GB available minimum (200 GB recommended) for the management server and a locally installed database.</p>
Display	<p>1024 x 768 or larger</p>
Operating system (desktop)	<ul style="list-style-type: none"> ■ Windows XP (32-bit, SP3; 64-bit, all SPs; all editions except Starter and Home; all patches applied, including Internet Explorer) ■ Windows 7 (32-bit, 64-bit; RTM and SP1; all editions except Starter and Home) ■ Windows 8 (32-bit, 64-bit) ■ Windows 8.1 (32-bit, 64-bit) ■ Windows 8.1 update for April (2014) (32-bit, 64-bit) ■ Windows 8.1 update for August (2014) (32-bit, 64-bit)

Table 2-4 Symantec Endpoint Protection Manager system requirements
(continued)

Component	Requirements
Operating system (server)	<ul style="list-style-type: none"> ■ Windows Server 2003 (32-bit, 64-bit; R2, SP1 or later; all patches applied, including Internet Explorer) ■ Windows Small Business Server 2003 (32-bit; all patches applied, including Internet Explorer) ■ Windows Server 2008 (32-bit, 64-bit; R2, RTM, SP1 and SP2) ■ Windows Small Business Server 2008 (64-bit) ■ 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)
Web browser	<ul style="list-style-type: none"> ■ Microsoft Internet Explorer 8, 9, 10, 11 ■ Mozilla Firefox 5.x through 38.0.1 ■ Google Chrome, through 42.0.2311.152 <p>For a list of supported browsers for Browser Intrusion Prevention, see: Supported Browser versions for Browser Intrusion Prevention</p>

Note: This Symantec Endpoint Protection Manager version manages clients earlier than version 12.1, regardless of the client operating system.

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

- SQL Server 2005, SP4
- SQL Server 2008, through SP3
- SQL Server 2008 R2, through SP2
- SQL Server 2012, through SP1
- SQL Server 2014

See [“Supported virtual installations and virtualization products”](#) on page 62.

System requirements for the Symantec Endpoint Protection client for Windows

Table 2-5 Symantec Endpoint Protection client for Windows system requirements

Component	Requirements
Processor	<ul style="list-style-type: none"> ■ 32-bit processor: 1 GHz Intel Pentium III or equivalent minimum (Intel Pentium 4 or equivalent recommended) ■ 64-bit processor: 2 GHz Pentium 4 with x86-64 support or equivalent minimum <p>Note: Itanium processors are not supported.</p>
Physical RAM	512 MB (1 GB recommended), or higher if required by the operating system
Hard drive	<p>1.8 GB of available hard disk space for the installation; additional space is required for content and logs</p> <p>Note: Space requirements are based on NTFS file systems.</p>
Display	800 x 600 or larger
Operating system (desktop)	<ul style="list-style-type: none"> ■ Windows XP Home or Professional (32-bit, SP3; 64-bit, all SPs) ■ Windows XP Embedded (SP3) ■ Windows Vista (32-bit, 64-bit) ■ Windows 7 (32-bit, 64-bit; RTM and SP1) ■ Windows 7 Embedded Standard ■ Windows 8 (32-bit, 64-bit) ■ Windows 8 Embedded (32-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 8.1 Embedded (32-bit) ■ <p>See “System requirements for the Symantec Endpoint Protection client for Windows Embedded” on page 56.</p>

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

Component	Requirements
Operating system (server)	<ul style="list-style-type: none"> ■ Windows Server 2003 (32-bit, 64-bit; R2, SP1 or later) ■ Windows Small Business Server 2003 (32-bit) ■ Windows Server 2008 (32-bit, 64-bit; R2, SP1, and SP2) ■ Windows Small Business Server 2008 (64-bit) ■ 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)

See [“Supported virtual installations and virtualization products”](#) on page 62.

System requirements for the Symantec Endpoint Protection client for Windows Embedded

Table 2-6 Symantec Endpoint Protection client for Windows Embedded system requirements

Component	Requirements
Processor	1 GHz Intel Pentium
Physical RAM	256 MB
Hard drive	450 MB of available hard disk space
Embedded operating system	<ul style="list-style-type: none"> ■ Windows Embedded Standard (WES) 2009 (32-bit, SP3) ■ Windows Embedded POSReady 2009 (32-bit, SP3) ■ Windows Embedded Point of Service (WEPOS) (32-bit, SP3) ■ Windows Embedded Standard 7 (32- and 64-bit) ■ Windows Embedded POSReady 7 (32- and 64-bit) ■ Windows Embedded Enterprise 7 (32- and 64-bit) ■ Windows Embedded 8 Standard (32- and 64-bit) ■ Windows Embedded 8.1 Industry Pro (32- and 64-bit) ■ Windows Embedded 8.1 Industry Enterprise (32- and 64-bit) ■ Windows Embedded 8.1 Pro (32- and 64-bit)

Table 2-6 Symantec Endpoint Protection client for Windows Embedded system requirements (*continued*)

Component	Requirements
Required minimum components	<ul style="list-style-type: none"> ■ Filter Manager (FitMgr.sys) ■ Performance Data Helper (pdh.dll) ■ Windows Installer Service ■ FBA: Driver Signing (applies only to XP-based Embedded) ■ WinLogon (applies only to XP-based Embedded)
Templates	<ul style="list-style-type: none"> ■ Application Compatibility (Default) ■ Digital Signage ■ Industrial Automation ■ IE, Media Player, RDP ■ Set Top Box ■ Thin Client <p>The Minimum Configuration template is not supported.</p> <p>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.</p>

For more information, see:

[Symantec Endpoint Protection support for Windows Embedded](#)

See “[About reduced-size client installation packages](#)” on page 114.

See “[Supported virtual installations and virtualization products](#)” on page 62.

System requirements for the Symantec Endpoint Protection client for Mac

Table 2-7 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	1 GB of available hard disk space for the installation
Display	800 x 600
Operating system	Mac OS X 10.8, 10.9, 10.10

System requirements for the Symantec Endpoint Protection client for Linux

Table 2-8 Symantec Endpoint Protection client for Linux system requirements

Component	Requirements
Hardware	<ul style="list-style-type: none"> ■ Intel Pentium 4 (2 GHz) or higher processor ■ 1 GB of RAM ■ 6 GB of available hard disk space
Operating systems	<ul style="list-style-type: none"> ■ CentOS 6U4, 6U5; 32-bit and 64-bit ■ Debian 6.0.5 Squeeze; 32-bit and 64-bit ■ Fedora 16, 17; 32-bit and 64-bit ■ Novell Open Enterprise Server (OES) 2 SP2 and 2 SP3 running SUSE Linux Enterprise Server (SLES) 10 SP3; 32-bit and 64-bit ■ Novell Open Enterprise Server (OES) 11 and 11 SP1 running SUSE Linux Enterprise Server (SLES) 11 SP1 and SP2; 64-bit ■ Oracle Linux (OEL) 5U8, 5U9, 6U2, 6U4, 6U5; 64-bit ■ Red Hat Enterprise Linux Server (RHEL) 5U7 - 5U10, 6U2 - 6U5, 7, 7.1; 32-bit and 64-bit ■ SUSE Linux Enterprise Server (SLES) 10 SP3, 10 SP4, 11 SP1 - 11 SP3; 32-bit and 64-bit ■ SUSE Linux Enterprise Desktop (SLED) 10 SP3, 10 SP4, 11 SP1 - 11 SP3; 32-bit and 64-bit ■ Ubuntu Server 11.10, 12.04, 12.04.2, 13.04; 64-bit ■ Ubuntu Desktop 11.10, 12.04, 12.04.2, 13.04; 64-bit <p>For a list of supported operating system kernels, see: Supported Linux kernels for Symantec Endpoint Protection</p>
Graphical desktop environments	<p>You can use the following graphical desktop environments to view the Symantec Endpoint Protection client's graphical user interface:</p> <ul style="list-style-type: none"> ■ KDE ■ Gnome

Table 2-8 Symantec Endpoint Protection client for Linux system requirements
(continued)

Component	Requirements
Other environmental requirements	<ul style="list-style-type: none"> ■ Oracle Java 1.5 or later; Java 7 or later recommended. This installation requires superuser privileges. ■ Unlimited Strength Java Cryptography Extension (JCE) You must install the Unlimited Strength Java Cryptography Extension policy files to match your version of Java. This installation requires superuser privileges. You can download the installation files under Additional Resources from the following Oracle website: http://www.oracle.com/technetwork/java/javase/downloads/index.html ■ i686-based dependent packages on 64-bit computers Many of the executable files in the Symantec Endpoint Protection client for Linux are 32-bit programs. For 64-bit computers, you must install the i686-based dependent packages before you install the Symantec Endpoint Protection client for Linux. 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 <code>sudo</code>: For Red Hat-based distributions: <code>sudo yum install glibc.i686 libgcc.i686 libX11.i686</code> For Debian-based distributions: <code>sudo apt-get install ia32-libs</code> For Ubuntu-based distributions: <code>sudo apt-get install libx11-6:i386 libgcc1:i386 libc6:i386</code>

See “Supported virtual installations and virtualization products” on page 62.

Internationalization requirements

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

Table 2-9 Internationalization requirements

Component	Requirements
Computer names, server names, and workgroup names	<p>Non-English characters are supported with the following limitations:</p> <ul style="list-style-type: none"> ■ 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	<p>English characters are required in the following situations:</p> <ul style="list-style-type: none"> ■ 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. <p>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.</p> <ul style="list-style-type: none"> ■ Push non-English characters to the client computers. <p>Some non-English characters that are generated on the server side may not appear properly on the client user interface.</p> <p>For example, a double-byte character set location name does not appear properly on non-double-byte character set named client computers.</p>
User Information client computer dialog box	<p>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.</p> <p>See “Collecting user information” on page 272.</p>
License Activation wizard	<p>Do not use double-byte characters in the following fields:</p> <ul style="list-style-type: none"> ■ First name ■ Last name ■ Company name ■ City ■ State/province <p>See “Activating or importing your Symantec Endpoint Protection 12.1.x product license” on page 96.</p>

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

Product license requirements

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

[Table 2-10](#) displays the requirements you need to license Symantec Endpoint Protection.

Table 2-10 Product license requirements

Product	Requirement
Paid license installation of Symantec Endpoint Protection	<p>A 60-day trial license is included with Symantec Endpoint Protection.</p> <p>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.</p> <p>See “About the licensing enforcement rules” on page 102.</p>
Symantec legacy virus protection software	<p>Symantec Endpoint Protection accepts the license file from your Symantec legacy virus protection software. You must purchase a new license when the legacy license expires.</p>

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 12.1.x product license”](#) on page 96.
- 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	<p>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.</p> <p>See “Activating or importing your Symantec Endpoint Protection 12.1.x product license” on page 96.</p>
Seat	<p>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.</p>
Trial license	<p>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.</p> <p>The evaluation period is 60 days from the initial installation of Symantec Endpoint Protection Manager.</p> <p>See “About purchasing licenses” on page 95.</p>
Over-deployed	<p>A license is over-deployed when the number of deployed clients exceeds the number of licensed seats.</p>

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 41.

See [“Licensing Symantec Endpoint Protection”](#) on page 92.

See [“About purchasing licenses”](#) on page 95.

See [“Activating or importing your Symantec Endpoint Protection 12.1.x product license”](#) on page 96.

Supported virtual installations and virtualization products

You use the Symantec Endpoint Protection clients to protect the supported operating systems that run in the virtual environments. You can also install and manage Symantec Endpoint Protection Manager on the supported operating systems that run in virtual environments. You install Symantec Endpoint Protection on the guest operating system, not the host.

[Table 2-11](#) lists the supported virtualization products.

Table 2-11 Supported virtualization products

Symantec software	Virtualization product
Symantec Endpoint Protection Manager, console, and embedded database components	<ul style="list-style-type: none"> ■ Windows 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 ■ Microsoft Virtual Server 2005 ■ Microsoft Enterprise Desktop Virtualization (MED-V), which includes Windows XP mode ■ Windows Server 2008 Hyper-V ■ Windows Server 2012 Hyper-V ■ Windows Server 2012 R2 Hyper-V ■ Citrix XenServer 5.6 or later ■ Virtual Box, supplied by Oracle
Symantec Endpoint Protection client software for Windows and Linux	<ul style="list-style-type: none"> ■ Windows 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 ■ Microsoft Virtual Server 2005 ■ Microsoft Enterprise Desktop Virtualization (MED-V), which includes Windows XP mode ■ Windows Server 2008 Hyper-V ■ Windows Server 2012 Hyper-V ■ Windows Server 2012 R2 Hyper-V ■ Citrix XenServer 5.6 or later ■ Virtual Box, supplied by Oracle

See [“Using Symantec Endpoint Protection in virtual infrastructures”](#) on page 635.

See [“Randomizing scans to improve computer performance in virtualized environments on Windows clients”](#) on page 473.

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 41.

About choosing a database type

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

Table 2-12 Databases that Symantec Endpoint Protection Manager uses

Database type	Description
Embedded database	<p>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.</p> <p>See “About basic management server settings” on page 65.</p>
SQL Server database	<p>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.</p> <p>You should consider purchasing and installing SQL Server for the following reasons:</p> <ul style="list-style-type: none"> ■ You must support more than 5,000 clients. Each management server that uses SQL Server can support up to 50,000 clients. If your organization has more than 50,000 clients, you can install another management server. ■ You want to support failover and load balancing. ■ You want to set up additional management servers as site partners. <p>See “About determining how many sites you need” on page 722.</p> <p>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.</p> <p>See “About SQL Server configuration settings” on page 68.</p>

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 74.

See [“Management server ports”](#) on page 67.

Table 2-13 Basic server settings

Setting	Default	Description
Site Name	My Site (default) Site <i>local host name</i> (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	<i>local host name</i>	The name of the computer that runs Symantec Endpoint Protection Manager.
Server data folder	C:\Program Files\Symantec Endpoint Protection Manager\data (32-bit operating system) C:\Program Files (x86)\Symantec Endpoint Protection Manager\data (64-bit operating system)	The directory in which the Symantec Endpoint Protection Manager places data files including backups, replicated logs, and other files. The installer creates this directory if it does not exist.
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 “Preparing for disaster recovery” on page 732.

Table 2-13 Basic server settings (*continued*)

Setting	Default	Description
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.

Management server ports

Symantec Endpoint Protection Manager uses the following ports by default. To change the default ports, choose the custom installation type when you run the Management Server Configuration Wizard.

All communication over these ports is sent over TCP.

See [“About basic management server settings”](#) on page 65.

Table 2-14 Symantec Endpoint Protection Manager ports

Setting	Default	Description
Server port	8443	Symantec Endpoint Protection Manager listens on this port.
Web console port	9090	Remote HTTP console connections use this port.
Client communications port	8014	The clients communicate with the management server on this port.
Remote management Web services port	8446	Remote Monitoring and Management (RMM) uses this port to send Web services traffic over HTTPS.
Server control port	8765	The Tomcat Web service uses this port.
Reporting port	8445	The Apache Web service uses this port for reporting.
Process launcher port	8447	The process launcher service uses this port to start those processes that require higher privileges on the management server.

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.

See [“Installing Symantec Endpoint Protection Manager”](#) on page 74.

Before you create the database, Symantec recommends that you install a new instance of SQL Server that conforms to Symantec installation and configuration requirements. You can install a database in an existing instance, but the instance must be configured properly or your database installation fails. For example, if you select a case-sensitive SQL collation, your installation fails.

Warning: Symantec Endpoint Protection Manager authenticates to SQL Server with a clear text database owner user name and password. To maximize the security posture of remote SQL Server communications, place both servers in the same secure subnet.

Table 2-15 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 72.
sa password	Set this password when you set Mixed Mode authentication.
Enabled protocol	TCP/IP
IP addresses for TCP/IP	Enable IP1 and IP2

Table 2-15 Required SQL Server configuration settings (*continued*)

Configuration setting	Installation requirement
TCP/IP port numbers for IP1, IP2, and IPALL	<p>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.</p> <p>The Symantec Endpoint Protection Manager database does not support dynamic ports.</p>
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 2-16](#) displays the settings that you might need to know before you begin the installation process.

Table 2-16 SQL Server database settings

Setting	Default	Description
Server name	<i>local host name</i>	Name of the computer that runs Symantec Endpoint Protection Manager.
Server data folder	C:\Program Files\Symantec Endpoint Protection Manager\data	Folder in which the Symantec Endpoint Protection Manager places data files including backups, replication, and other Symantec Endpoint Protection Manager files. The installer creates this folder if it does not exist.

Table 2-16 SQL Server database settings (*continued*)

Setting	Default	Description
Encryption password	None	<p>The password that encrypts communication between Symantec Endpoint Protection Manager and clients. The password can be from 6-32 alphanumeric characters and is required.</p> <p>Document this password and put it in a secure location. You cannot change or recover the password after you create the database. You must also enter this password for disaster recovery purposes if you do not have a backed-up database to restore.</p> <p>See “Performing disaster recovery” on page 737.</p>
Database server	<i>local host name</i>	<p>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 <i>host name</i> or the host's <i>IP address</i>. If the database server was installed with a named instance, type either <i>host name\instance_name</i> or <i>IP address\instance_name</i>. The use of <i>host name</i> only works with properly configured DNS.</p> <p>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.</p>
SQL Server Port	1433	<p>The port that is used to send and receive traffic to the SQL Server.</p> <p>The use of port 0 is not supported. Port 0 specifies a random, negotiated port.</p>
Database Name	sem5	Name of the database that is created.
Database user name	sem5	<p>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.</p>

Table 2-16 SQL Server database settings (*continued*)

Setting	Default	Description
Database password	None	The password that is associated with the database user account. The name can be a combination of alphanumeric values and the special characters ~ # % _ + = : . / . The special characters ! @ * () { } [] ; , ? are not allowed.
SQL Server client folder	SQL Server 2005: <i>Install Directory\90\Tools\Binn</i> SQL Server 2008: <i>Install Directory\100\Tools\Binn</i> SQL Server 2012: <i>Install Directory\110\Tools\Binn</i> SQL Server 2014: <i>Install Directory\Client SDK\ODBC\110\Tools\Binn</i>	Location of the local SQL Client Utility directory that contains bcp.exe. <i>Installation Directory</i> represents the installation location of Microsoft SQL Server. By default, this location is C:\Program Files\Microsoft SQL Server\.
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 2-16 SQL Server database settings (*continued*)

Setting	Default	Description
Database data folder	<p>Automatically detected after you click Default.</p> <p>SQL Server 2005: <i>Install Directory</i>\MSSQL.1\MSSQL\Data</p> <p>SQL Server 2008: <i>Install Directory</i>\MSSQL10.MSSQLSERVER\MSSQL\Data</p> <p>SQL Server 2008 R2: <i>Install Directory</i>\MSSQL10_50.MSSQLSERVER\MSSQL\Data</p> <p>SQL Server 2012: <i>Install Directory</i>\MSSQL11.MSSQLSERVER\MSSQL\Data</p> <p>SQL Server 2014: <i>Install Directory</i>\MSSQL12.MSSQLSERVER\MSSQL\Data</p>	<p>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.</p> <p><i>Installation Directory</i> represents the installation location of Microsoft SQL Server. By default, this location is C:\Program Files\Microsoft SQL Server\.</p> <ul style="list-style-type: none"> ■ If you install to a named instance on SQL Server 2005, the instance name is appended to MSSQL with a dot numeric identifier. For example, \MSSQL.n\MSSQL\Data ■ If you install to a named instance on SQL Server 2008, the instance name is appended to MSSQL10. For example, \MSSQL10.<i>instance name</i>\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.<i>instance name</i>\MSSQL\Data ■ If you install to a named instance on SQL Server 2012, the instance name is appended to MSSQL11. For example, \MSSQL11.<i>instance name</i>\MSSQL\Data ■ If you install to a named instance on SQL Server 2014, the instance name is appended to MSSQL12. For example, \MSSQL12.<i>instance name</i>\MSSQL\Data <p>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.</p>

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 68.

Installing Symantec Endpoint Protection Manager

This chapter includes the following topics:

- [Installing Symantec Endpoint Protection Manager](#)
- [Configuring Symantec Endpoint Protection Manager during installation](#)
- [Uninstalling Symantec Endpoint Protection Manager](#)
- [Logging on to the Symantec Endpoint Protection Manager console](#)
- [What you can do from the console](#)
- [What do I do after I install the management server?](#)

Installing Symantec Endpoint Protection Manager

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

Note: You may need to edit the security policies to allow the virtual service accounts to run correctly for Windows 7 / Server 2008 R2 or later. Earlier operating systems are not affected, but require Network Service to be present in security policies.

As of 12.1.6, the Symantec Endpoint Protection Manager installation automatically changes local security policies to grant the correct user rights to Symantec Endpoint Protection Manager virtual service accounts. If domain policies do not comply with the required user rights, a warning appears with more information and identifies which domain policies you must change. A warning also appears if the domain policies cannot be read.

For more information, see:

[How to assign user rights to the Windows Security Policies for Symantec Endpoint Protection Manager services](#)

Note: Symantec Endpoint Protection Manager requires full access to the system registry for installation and normal operation. To prepare a Windows Server 2003 computer on which you plan to remotely install Symantec Endpoint Protection Manager, you must first allow remote control on the computer. When you connect with Remote Desktop, you must also use a console session or shadow the console session in Remote Desktop.

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

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](#).

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 during installation”](#) on page 76.
- 8 You configure the management server according to your requirements. Follow the on-screen instructions to specify the type of configuration, the settings for the administrator and for mail server communications. You also choose whether 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.

After the server and the database configuration, click **Next** to create the database.

See [“About choosing a database type”](#) on page 65.
- 9 Click **Finish** to complete the 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 in, you can begin client deployment.

See [“Logging on to the Symantec Endpoint Protection Manager console”](#) on page 78.

See [“About client installation methods”](#) on page 115.

See [“Preparing for client installation”](#) on page 108.

See [“Getting up and running on Symantec Endpoint Protection for the first time”](#) on page 41.

Configuring Symantec Endpoint Protection Manager during installation

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

See [“Installing Symantec Endpoint Protection Manager”](#) on page 74.

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

To configure the server, you specify the following information:

- The configuration type, which is **Default configuration** or **Custom configuration**. The wizard provides information about each type.
- Whether you want to use a recovery file.

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

See [“Performing disaster recovery”](#) on page 737.

- The password for the default administrator account.
- The email address that receives important notifications and reports.
- The mail server name and port number.
- The Symantec Sales Partner information, if a partner manages your Symantec licenses.

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

Uninstalling Symantec Endpoint Protection Manager

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

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

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

To uninstall Symantec Endpoint Protection Manager

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

- 1 On the server computer, on the **Start** menu, click **Control Panel > Add or Remove Programs** (or **Control Panel > Programs > Uninstall a program**).
- 2 In the **Add or Remove Programs** (or **Uninstall or change a program**) dialog box, click **Symantec Endpoint Protection Manager**, and then click **Change, Remove, or Uninstall**.
- 3 Follow the onscreen prompts to remove Symantec Endpoint Protection Manager.

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

For more information, see [Uninstall Symantec Endpoint Protection](#).

See [“Backing up the database and logs”](#) on page 733.

See [“Turning off replication before an upgrade from Symantec Endpoint Protection 11.0”](#) on page 155.

See [“Turning on replication after an upgrade from Symantec Endpoint Protection 11.0”](#) on page 155.

Logging on to the Symantec Endpoint Protection Manager console

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

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

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

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

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.

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 stand-alone Web browser”](#) on page 603.

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 time period for staying logged on to the console”](#) on page 85.

To log on to the console locally

- 1 Go to **Start > Programs > Symantec Endpoint Protection Manager > Symantec Endpoint Protection Manager**.
- 2 In the **Symantec Endpoint Protection Manager** logon dialog box, type the user name (`admin` by default) and the password that you configured during the installation.

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

- 3 Optionally check **Remember my user name**, **Remember my password** or both, if available, and then click **Log On**.

See [“Displaying the Forgot your password? link so that administrators can reset lost passwords”](#) on page 307.

To log on to the console remotely

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

http://*host name*:9090

where *host name* is the host name or IP address of the management server. For a list of supported web browsers, see [Release Notes and System Requirements for all versions of Symantec Endpoint Protection and Symantec Network Access Control](#).

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

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

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

The 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 83.

See [“Displaying a message for administrators to see before logging on to the Symantec Endpoint Protection Manager console”](#) on page 82.

See [“About accepting the self-signed server certificate for Symantec Endpoint Protection Manager”](#) on page 81.

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 Symantec Technical Support knowledge base article, [How to install the certificate for Symantec Endpoint Protection Manager for Web console access](#).

See [“Logging on to the Symantec Endpoint Protection Manager console”](#) on page 78.

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”](#) on page 295.

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 is prepopulated on the logon screen.

To display the Remember my user name and Remember my password check boxes on the logon screen

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

- 3 Under **Domains**, select the domain for which to allow administrators to save logon credentials.
- 4 Click **Edit Domain Properties**.
- 5 On the **Passwords** tab, check **Allow users to save credentials when logging on**.
- 6 Click **OK**.

See [“Resetting a forgotten Symantec Endpoint Protection Manager password”](#) on page 306.

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”](#) on page 295.

See [“Logging on to the Symantec Endpoint Protection Manager console”](#) on page 78.

Configuring an administrator's account to lock 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 configure an administrator's account to lock 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 306.

See [“Changing the password for an administrator account”](#) on page 305.

See [“Enabling Symantec Endpoint Protection Manager logon passwords to never expire”](#) on page 308.

Changing the time period for staying logged on to the console

To help protect the console, the console requires you to reenter your user name and password after one hour. To increase security, you can decrease the timeout period before you must log on to the management console.

In version 12.1.4 and earlier, you can set the time period to **Never**.

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

- 1 In the console, click **Admin**, and then click **Servers**.
- 2 Click **Local Site** or a remote site and click **Edit Site Properties**.
- 3 On the **General** tab, click the **Console Timeout** drop-down list and select one of the available options for length of time.
- 4 Click **OK**.

What you can do from the console

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

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

Table 3-1 Symantec Endpoint Protection Manager console pages

Page	Description
Home	<p>Display the security status of your network.</p> <p>You can do the following tasks from the Home page:</p> <ul style="list-style-type: none">■ Obtain a count of detected viruses and other security risks.■ Obtain a count of unprotected computers in your network.■ Obtain a count of computers that received virus definition and other content updates.■ View license status.■ Adjust console preferences.■ Get information about the latest Internet and security threats. <p>See “Configuring reporting preferences” on page 602.</p> <p>See “Checking the license status in Symantec Endpoint Protection Manager” on page 101.</p>
Monitors	<p>Monitor event logs that concern Symantec Endpoint Protection Manager and your managed computers.</p> <p>You can do the following tasks from the Monitors page:</p> <ul style="list-style-type: none">■ View risk distribution graphs.■ View event logs.■ View the status of recently issued commands.■ View and create notifications. <p>See “Viewing and acknowledging notifications” on page 628.</p>
Reports	<p>Run reports to get up-to-date information about computer and network activity.</p> <p>You can do the following tasks from the Reports page:</p> <ul style="list-style-type: none">■ Run Quick Reports.■ Run the Daily Summary Report.■ Run the Weekly Summary Report. <p>See “Running and customizing quick reports” on page 606.</p>

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

Page	Description
Policies	<p>Display the security policies that define the protection technology settings.</p> <p>You can do the following tasks from the Policies page:</p> <ul style="list-style-type: none"> ■ View and adjust the protection settings. ■ Create, edit, copy, and delete security policies. ■ Assign security policies to computer groups. ■ Configure LiveUpdate settings for client computers. <p>See “The types of security policies” on page 318.</p> <p>See “Performing the tasks that are common to all policies” on page 315.</p> <p>See “Managing content updates” on page 181.</p>
Clients	<p>Manage computers and groups.</p> <p>You can do the following tasks from this page:</p> <ul style="list-style-type: none"> ■ Create and delete groups. ■ Edit group properties. ■ View the security policies that are assigned to groups. ■ Run commands on groups. ■ Assign the client software to computers in your network. <p>See “Managing groups of clients” on page 236.</p>

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

Page	Description
Admin	<p>Manage Symantec Endpoint Protection Manager settings, licenses, and administrator accounts.</p> <p>You can do the following tasks from the Admin page:</p> <ul style="list-style-type: none"> ■ Change the time that you are logged on to Symantec Endpoint Protection Manager. ■ Create, edit, and delete administrator accounts. ■ View and edit email and proxy server settings. ■ Import and purchase licenses. ■ Adjust the LiveUpdate schedule for Symantec Endpoint Protection Manager. ■ Download content updates from LiveUpdate. ■ View LiveUpdate status and recent downloads. ■ Manage Symantec Endpoint Protection Manager domains. ■ Add, delete, and export client install packages. <p>See "Changing the time period for staying logged on to the console" on page 85.</p> <p>See "Managing administrator accounts" on page 291.</p> <p>See "Managing content updates" on page 181.</p>

What do I do after I install the management server?

[Table 3-2](#) displays the tasks to perform after you install and configure the product to assess whether the client computers have the correct level of protection.

Table 3-2 Tasks to perform two weeks after you install

Action	Description
Modify the Virus and Spyware Protection policy	Change the following default scan settings: <ul style="list-style-type: none"> ■ 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 422. ■ Enable Risk Tracer in Auto-Protect. For more information, see the knowledge base article: What is Risk Tracer? Risk Tracer has the following prerequisites: <ul style="list-style-type: none"> ■ Network Threat Protection is enabled. See “Running commands on client computers from the console” on page 261. ■ Windows File and Printer Sharing is enabled. See “Customizing Auto-Protect for Windows clients” on page 464.
Modify the Firewall policy for the remote computers group and the servers group	<ul style="list-style-type: none"> ■ Increase the security for remote computers by making sure that the following default firewall rules for an off-site location are enabled: <ul style="list-style-type: none"> ■ 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 370. See “Managing locations for remote clients” on page 276.

Table 3-2 Tasks to perform two weeks after you install (*continued*)

Action	Description
<p>Exclude applications and files from being scanned</p>	<p>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.</p> <p>For more information, see the knowledge base article: About the automatic exclusion of files and folders for Microsoft Exchange server and Symantec products.</p> <p>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.</p> <p>For more information, see the knowledge base article: How to exclude MS SQL files and folders using Centralized Exceptions.</p> <p>You can also exclude files by extension for Auto-Protect scans on Windows computers.</p> <p>See “Creating exceptions for Virus and Spyware scans” on page 498.</p> <p>See “Customizing Auto-Protect for Windows clients” on page 464.</p> <p>See “Customizing Auto-Protect for Mac clients” on page 465.</p>
<p>Run a quick report and scheduled report after the scheduled scan</p>	<p>Run the quick reports and scheduled reports to see whether the client computers have the correct level of security.</p> <p>See “About the types of reports” on page 604.</p> <p>See “Running and customizing quick reports” on page 606.</p> <p>See “How to generate scheduled reports” on page 609.</p>
<p>Check to ensure that scheduled scans have been successful and clients operate as expected</p>	<p>Review monitors, logs, and the status of client computers to make sure that you have the correct level of protection for each group.</p> <p>See “Monitoring endpoint protection” on page 593.</p>

Table 3-2 Tasks to perform two weeks after you install (*continued*)

Action	Description
<p>Assess your content storage and client communication bandwidth requirements</p>	<p>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.</p> <p>If your environment must control network bandwidth precisely, you can also throttle client communication. For more information, see the knowledge base article: Symantec Endpoint Protection Bandwidth Control for Client Communication</p> <p>See “Managing content updates” on page 181.</p> <p>For more information about calculating storage and bandwidth needs, see the Symantec Endpoint Protection Sizing and Scalability Best Practices White Paper.</p>
<p>Configure notifications for a single risk outbreak and when a new risk is detected</p>	<p>Create a notification for a Single risk event and modify the notification for Risk Outbreak.</p> <p>For these notifications, Symantec recommends that you do the following actions:</p> <ol style="list-style-type: none"> 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. <p>Notifications are critical to maintaining a secure environment and can also save you time.</p> <p>See “Setting up administrator notifications” on page 630.</p> <p>See “Managing notifications” on page 620.</p>

See “[Getting up and running on Symantec Endpoint Protection for the first time](#)” on page 41.

See the knowledge base article: [Symantec Endpoint Protection Recommended Best Practices for Securing an Enterprise Environment](#)

Managing product licenses

This chapter includes the following topics:

- [Licensing Symantec Endpoint Protection](#)
- [About the trial license](#)
- [About purchasing licenses](#)
- [Activating or importing your Symantec Endpoint Protection 12.1.x product license](#)
- [About product upgrades and licenses](#)
- [About renewing your Symantec Endpoint Protection license](#)
- [Checking the license status in Symantec Endpoint Protection Manager](#)
- [About the licensing enforcement rules](#)
- [Backing up your license files](#)
- [Recovering a deleted license](#)
- [Purging obsolete clients from the database to make more licenses available](#)
- [About multi-year licenses](#)
- [Licensing an unmanaged Windows client](#)

Licensing Symantec Endpoint Protection

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

You use the License Activation Wizard to activate new or renewed licenses, or when you convert a trial license to a paid license. You license Symantec Endpoint

Protection according to the number of clients that you need to protect the endpoints at your site.

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

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

See [“About administrator account roles and access rights”](#) on page 293.

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

Table 4-1 Licensing tasks

Task	Description
Check the product license requirements	<p>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, security content, and product updates from LiveUpdate.</p> <p>See “Product license requirements” on page 61.</p> <p>See “About the licensing enforcement rules” on page 102.</p> <p>See “About multi-year licenses” on page 105.</p>
Purchase a license and save it to the management server	<p>You need to purchase a license in the following situations:</p> <ul style="list-style-type: none"> ■ You want to purchase Symantec Endpoint Protection. ■ Your trial license expired. ■ Your paid license expired. ■ Your license is over-deployed. ■ Your upgrade license from 11.0 expired. <p>You do not need to manually download a license file. After you purchase your license, you receive an email with a Symantec license file (.sif) or a license serial number.</p> <p>See “About purchasing licenses” on page 95.</p> <p>See “Checking the license status in Symantec Endpoint Protection Manager” on page 101.</p> <p>See “About the trial license” on page 94.</p>

Table 4-1 Licensing tasks (*continued*)

Task	Description
<p>Import the license file and activate your purchased license</p>	<p>You use the License Activation Wizard in the Symantec Endpoint Protection Manager console to import and activate your Symantec product license.</p> <p>Before you activate the license, you must have one of the following items:</p> <ul style="list-style-type: none"> ■ A Symantec license serial number ■ A Symantec license file (.slf) <p>You receive one or the other of these when you purchase a license.</p> <p>See “Activating or importing your Symantec Endpoint Protection 12.1.x product license” on page 96.</p> <p>See “About the Symantec Licensing Portal” on page 100.</p>
<p>Back up your license files</p>	<p>Back up your license files to preserve them in case the database or the computer’s hard disk becomes damaged.</p> <p>See “Backing up your license files” on page 103.</p> <p>See “Recovering a deleted license” on page 103.</p>
<p>Review the preconfigured license notifications</p>	<p>Preconfigured license notifications alert administrators about expired licenses and other license issues.</p> <p>See “What are the types of notifications and when are they sent?” on page 622.</p>
<p>Keep track of when your licenses expire, and renew your licenses</p>	<p>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.</p> <p>See “Checking the license status in Symantec Endpoint Protection Manager” on page 101.</p> <p>See “About renewing your Symantec Endpoint Protection license” on page 101.</p>

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 licenses”](#) on page 95.

About purchasing 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.
- You decide to keep the new version after the upgrade trial from 11.0 expires. If you use 11.0, Symantec sends you an email with an upgrade offer that includes a free upgrade trial. If you decide to keep the new version beyond the upgrade trial period of 90 days, you need to purchase a paid license.

Depending upon how you purchase your license, you receive 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 4-2](#) displays where to learn more about purchasing licenses.

Table 4-2 Purchasing license tasks

Task	Description
Determine your licensing requirements	See “ Product license requirements ” on page 61. See “ About the licensing enforcement rules ” on page 102.
Find out where to buy product licenses	You can purchase a Symantec product license from the following sources: <ul style="list-style-type: none"> ■ The Symantec online store: http://store.symantec.com/ ■ Your preferred Symantec reseller: To find a reseller, use the Partner locator. To find out more about Symantec partners, go to http://www.symantec.com/partners/index.jsp ■ The Symantec sales team: Visit the Symantec Ordering 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 94.
Get help with purchasing licenses or learn more about licenses	http://customercare.symantec.com/

See “[Licensing Symantec Endpoint Protection](#)” on page 92.

Activating or importing your Symantec Endpoint Protection 12.1.x 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.
- Activating a license after you upgrade from a previous version, such as 11.0.

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

- Symantec Licensing Portal

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

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

- The Welcome screen that appears after you install the product.
- From the **Common Tasks** menu on the **Home** page.
- The **Admin** page of the Symantec Endpoint Protection Manager console.

If you activate or import your license from the Welcome screen or the **Common Tasks** menu, you can skip to step [3](#).

To activate or import your Symantec Endpoint Protection 12.1.x 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	<p>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.</p> <p>If you are an eFlex (Symantec Enterprise Options) customer and have an eFlex-generated serial number, select I have a Symantec License File.</p>
I have a Symantec License File (.sif)	<p>In most cases, you receive a Symantec license file (.sif 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 .sif file, select this option.</p> <p>Note: You must extract the .sif file from the .zip file before you can use it to activate your product license.</p> <p>Warning: The .sif 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.</p>

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**.
 - If you selected **I have a Symantec License File (.sif)**, click **Add File**. Browse to and select the .sif 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 94.

See [“About renewing your Symantec Endpoint Protection license”](#) on page 101.

See [“About purchasing licenses”](#) on page 95.

See [“Licensing Symantec Endpoint Protection”](#) on page 92.

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 4-3](#) includes the information you need.

Table 4-3 Licensing contact information

Type of information	Description
Technical Contact	Contact information for the person who is in charge of the technical activities that are concerned with installing or maintaining your endpoint security infrastructure. The contact's name, email address, and phone number are required.
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 92.

About the Symantec Licensing Portal

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

The Symantec Licensing Portal is now part of MySymantec. You can access the Licensing Portal through the following website:

<https://licensing.symantec.com>

Note: If you have existing credentials for MySymantec, you can use those credentials to access licensing information. If you do not have a MySymantec account, you must create one before you can use the Licensing Portal. To create an account, go to the Licensing Portal website and then click **Register Now**.

The Symantec Customer Care website has additional information about using the Symantec Licensing Portal to manage licenses:

<http://customersupport.symantec.com/>

See “[Activating or importing your Symantec Endpoint Protection 12.1.x product license](#)” on page 96.

See “[Licensing Symantec Endpoint Protection](#)” on page 92.

About product upgrades and licenses

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

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

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

See “[Upgrading to a new release](#)” on page 145.

See “[Licensing Symantec Endpoint Protection](#)” on page 92.

About renewing your Symantec Endpoint Protection license

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

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

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

See [“About purchasing licenses”](#) on page 95.

See [“Activating or importing your Symantec Endpoint Protection 12.1.x product license”](#) on page 96.

See [“Recovering a deleted license”](#) on page 103.

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 determine if your installation uses a paid license or a trial license

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

To check license status for paid licenses

- 1 In the console, click **Home**.
 - 2 On the **Home** page, click **Licensing Details**.
- See [“Licensing Symantec Endpoint Protection”](#) on page 92.
- See [“Activating or importing your Symantec Endpoint Protection 12.1.x product license”](#) on page 96.

About the licensing enforcement rules

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

Table 4-4 Licensing enforcement rules

Where applies	Rule
Term of license	<p>The term of the license starts from the time and date of activation until midnight of the last day of the licensing term.</p> <p>If you have multiple sites, the license expires on the day and the time of the westernmost Symantec Endpoint Protection Manager database.</p>
License coverage: Symantec Endpoint Protection components	<p>A Symantec Endpoint Protection license applies to the Symantec Endpoint Protection clients. For instance, in a network with 50 endpoints, the license must provide for a minimum of 50 seats. Instances of Symantec Endpoint Protection Manager do not require a license.</p>
License coverage: sites and domains	<p>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.</p> <p>If you have not implemented replication, you may deploy the same .sif 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.</p>
License coverage: platforms	<p>Licensing seats apply to clients running on any platform, whether the platform is Windows, Mac, or Linux.</p>

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

Where applies	Rule
License coverage: products and versions	License seats apply equally across product versions. For example, a license covers both version 11.0 and 12.1.x clients within the same site.

See [“Licensing Symantec Endpoint Protection”](#) on page 92.

Backing up your license files

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

By default, when you import the license file using the Licensing Activation Wizard, Symantec Endpoint Protection Manager places a copy of the license file in the following location: *Symantec Endpoint Protection Manager installation directory\lnetpub\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 12.1.x product license”](#) on page 96.

See [“About the Symantec Licensing Portal”](#) on page 100.

See [“Licensing Symantec Endpoint Protection”](#) on page 92.

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 [“Configuring a separate purge interval for offline non-persistent VDI clients”](#) on page 678.

See [“Licensing Symantec Endpoint Protection”](#) on page 92.

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 103.

See [“Licensing Symantec Endpoint Protection”](#) on page 92.

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.

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

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

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

- 4 Check that the .slf file is in either one of the following folders:
 - For the clients that run on a pre-Vista version of Windows: *Drive:\Documents and Settings\All Users\Application Data\Symantec\Symantec Endpoint Protection\CurrentVersion\Data\Config*
 - For the clients that run on Vista or a later version of Windows: *Drive:\ProgramData\Symantec\Symantec Endpoint Protection\CurrentVersion\Data\Config*

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

See [“Enabling or disabling client submissions to Symantec Security Response”](#) on page 442.

Installing the Symantec Endpoint Protection client

This chapter includes the following topics:

- [Preparing for client installation](#)
- [About client installation methods](#)
- [Exporting client installation packages](#)
- [About the Windows client installation settings](#)
- [Configuring Windows client installation feature sets](#)
- [Configuring client packages to uninstall existing third-party security software](#)
- [Restarting the client computers from Symantec Endpoint Protection Manager](#)
- [Installing the Symantec Endpoint Protection client for Mac](#)
- [Installing the Symantec Endpoint Protection client for Linux](#)
- [About managed and unmanaged clients](#)
- [Installing an unmanaged Windows client](#)
- [Uninstalling the Symantec Endpoint Protection client for Windows](#)
- [Uninstalling the Symantec Endpoint Protection client for Mac](#)
- [Uninstalling the Symantec Endpoint Protection client for Linux](#)
- [Managing client installation packages](#)
- [Adding client installation package updates](#)

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 5-1](#) lists the actions that you must perform to install the client software on the computers in your network.

Table 5-1 Client computer preparation

Action	Description
Identify client computers	<p>Identify the computers on which you want to install the client software. Check that all the computers run a supported operating system.</p> <p>Note: Symantec recommends that you also install the client on the computer that hosts Symantec Endpoint Protection Manager.</p> <p>For the most current system requirements, see: Release Notes and System Requirements for all versions of Symantec Endpoint Protection and Symantec Network Access Control</p>
Identify computer groups (optional)	<p>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.</p> <p>You can also import an existing group structure such as an Active Directory structure.</p> <p>See "Managing groups of clients" on page 236.</p> <p>See "Importing existing groups and computers from an Active Directory or an LDAP server" on page 240.</p> <p>See "Assigning clients to groups before you install the client software" on page 246.</p>

Table 5-1 Client computer preparation (*continued*)

Action	Description
Prepare client computers for deployment and installation	<p>Prepare the computers for remote client deployment and for successful communication with Symantec Endpoint Protection Manager after installation.</p> <ul style="list-style-type: none">■ Modify any existing firewall settings to allow communication during Remote Push deployment, and between Symantec Endpoint Protection components after 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 “About the communication ports that Symantec Endpoint Protection uses” on page 113. See “Installing clients with Remote Push” on page 120. See “Preparing Windows and Mac computers for remote deployment” on page 111.■ Uninstall any legacy Symantec virus protection software, such as Symantec AntiVirus or Symantec Client Security. Migration directly from these legacy 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.■ Uninstall third-party security software on all operating systems. For Windows operating systems, you can configure client packages to automatically uninstall existing third-party security software when you prepare to deploy clients. Note: Some programs may have special uninstallation routines. See the documentation for the third-party software. See “Configuring client packages to uninstall existing third-party security software” on page 127.

Table 5-1 Client computer preparation (*continued*)

Action	Description
Determine features and deploy client software	<p>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.</p> <p>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.</p> <p>See “About client installation methods” on page 115.</p> <p>See “Exporting client installation packages” on page 124.</p> <p>See “Installing Windows client software using third-party tools” on page 789.</p> <ul style="list-style-type: none"> ■ 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. <p>See “Which features should you install on the client?” on page 117.</p> <p>See “About the Windows client installation settings” on page 126.</p> <p>See “Configuring Windows client installation feature sets” on page 127.</p> ■ For Windows clients, you can choose to automatically uninstall existing third-party security software when you configure client installation settings. <p>See “Configuring client packages to uninstall existing third-party security software” on page 127.</p>
Verify installation status	<p>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.</p> <p>See “How to determine whether the client computer is connected and protected” on page 169.</p> <p>See “Restarting the client computers from Symantec Endpoint Protection Manager” on page 129.</p>

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 41.

Preparing Windows and Mac computers for remote deployment

Table 5-2 lists the tasks that you must do on Windows operating systems to successfully install the client remotely. See your Windows documentation for more information on any tasks you do not know how to perform.

Table 5-3 lists the tasks that you must do on Mac operating systems to successfully install the Symantec Endpoint Protection client remotely. See your Mac documentation for more information on any tasks you do not know how to perform.

Table 5-2 Windows remote deployment preparation tasks

Operating system	Tasks
<p>Prepare Windows XP computers and Windows Server 2003 servers that are installed in workgroups</p>	<p>Windows XP computers and Windows Server 2003 servers that are installed in workgroups do not accept remote deployment by default. To permit remote deployment, disable Simple File Sharing.</p> <p>Note: This limitation does not apply to computers that are part of an Active Directory domain.</p> <p>You may also need to perform the following tasks:</p> <ul style="list-style-type: none"> ■ Ensure that the Administrator account does not have a blank password. ■ Disable the Windows Firewall, or allow the required ports for communication between the client and Symantec Endpoint Protection Manager.
<p>Prepare Windows Vista, Windows 7, or Windows Server 2008 / 2008 R2 computers</p>	<p>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.</p> <p>To disable UAC remote restrictions, see: http://support.microsoft.com/kb/951016</p> <p>If the Windows client computer is part of an Active Directory domain, use domain administrator account credentials with local administrator privileges for remote push.</p> <p>Perform the following tasks:</p> <ul style="list-style-type: none"> ■ Disable the Windows Firewall, or configure the firewall to allow the required traffic. ■ Disable the Sharing Wizard. ■ Enable network discovery by using the Network and Sharing Center. ■ Enable the built-in administrator account and assign a password to the account. ■ Verify that the account has administrator privileges. ■ Disable or remove Windows Defender.

Table 5-2 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	<p>Before you deploy, perform the following tasks:</p> <ul style="list-style-type: none"> ■ Disable the Windows Firewall, or configure the firewall to allow the required traffic. ■ 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 5-3 Mac remote deployment preparation tasks

Operating system	Tasks
Prepare the Mac computers on any supported operating system	<p>Before you deploy, perform the following tasks on the Mac computers:</p> <ul style="list-style-type: none"> ■ 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 Apple knowledge base article that applies to your version of the Mac operating system. OS X Mountain Lion: Prevent others from discovering your computer (10.8) OS X Mavericks: Prevent others from discovering your Mac (10.9) OS X Yosemite: Prevent others from discovering your Mac (10.10) ■ Ensure that the firewall does not block the port that Secure Shell (SSH) uses, which is by default TCP port 22. This port allows the required communication for remote login. ■ Uninstall any third-party virus protection software suites. See the documentation for the third-party software. <p>If the Mac 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 Mac to which you deploy.</p>

See [“About the communication ports that Symantec Endpoint Protection uses”](#) on page 113.

See [“Installing clients with Remote Push”](#) on page 120.

See [“Preparing for client installation”](#) on page 108.

About the communication ports that Symantec Endpoint Protection uses

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

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

Table 5-4 Ports for client and server installation and communication

Function	Component	Protocol and port
Push deployment	Management server and client	TCP 139 and 445 on management servers and clients UDP 137 and 138 on management servers and clients TCP ephemeral ports on management servers and clients TCP 22 on Mac clients
Group Update Provider communication	Management server and Group Update Provider Group Update Provider and clients	TCP 2967 on all devices Note: You can change this default port.
General communication	Management server and client	For management servers and clients: <ul style="list-style-type: none"> ■ TCP 8014 for management servers, by default. You can change TCP 8014 (HTTP) to TCP 443 (HTTPS). ■ TCP ephemeral port on clients. For remote management servers and consoles: <ul style="list-style-type: none"> ■ TCP 8443 for remote management servers and console ■ TCP ephemeral ports and 9090 on consoles ■ TCP 8445 for remote reporting consoles
Replication communication	Site to site between database servers	TCP 8443 between database servers

Table 5-4 Ports for client and server installation and communication
(continued)

Function	Component	Protocol and port
Remote Symantec Endpoint Protection Manager console installation	Management server and remote management server console	TCP 9090 on remote management servers TCP ephemeral ports on remote consoles Note: You can change the port.
Web services	Remote Monitoring and Management (RMM)	TCP 8446 for RMM Web services
External database communication	Remote SQL Server and management server	TCP 1433 on remote SQL Server TCP ephemeral ports on management servers Note: Port 1433 is the default port.
LiveUpdate	LiveUpdate client and server	TCP ephemeral ports on clients TCP 80 on LiveUpdate servers

- 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 [“Enabling and disabling a firewall policy”](#) on page 342.

See [“Monitoring endpoint protection”](#) on page 593.

See [“Preparing for client installation”](#) on page 108.

About reduced-size client installation packages

Symantec Endpoint Protection 12.1.6 introduces options for a reduced-size installation package for Windows Embedded clients and virtual desktop infrastructure (VDI) clients. The reduced-size client is approximately 80 percent to 90 percent smaller on disk than standard-size Windows clients.

The reduced-size package keeps the size of the installation down in the following ways:

- The reduced-size client package uses reduced-size virus and spyware definitions. The reduced-size definitions are a fixed size and include the most recent set of definitions only, rather than the standard set of definitions. LiveUpdate downloads this content to Symantec Endpoint Protection Manager by default. The reduced-size content provides slightly less Virus and Spyware Protection than the standard-size content. Symantec recommends that you install and enable all protection technologies to mitigate this small reduction in Virus and Spyware Protection. These protection technologies include the firewall, Download Insight, Intrusion Prevention, and SONAR. Symantec also recommends that you use system lockdown to ensure the highest level of security.
- 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 reduced-size client employs NTFS compression on more folders than the standard-sized client.

You deploy the reduced-size installation package by using the same methods that you deploy the standard-size installation package. In the **Client Deployment Wizard**, you choose **Default Reduced Size Installation Settings** for the client install settings. You choose this same option if you export an installation package through **Admin > Install Packages > Client Install Package**.

If you configure embedded images for Windows Embedded Standard 7 and later with templates, all templates except for **Minimum Configuration** work well with Symantec Endpoint Protection. The supported write filter is the File Based Write Filter (FBWF) with the Registry Filter. If the write filter status is incompatible with the installation, the Symantec Endpoint Protection installer alerts you to the changes you need to make.

[Symantec Endpoint Protection support for Windows Embedded](#)

See [“System requirements for the Symantec Endpoint Protection client for Windows Embedded”](#) on page 56.

See [“About client installation methods”](#) on page 115.

See [“Exporting client installation packages”](#) on page 124.

See [“Configuring a site to download content updates”](#) on page 189.

See [“Configuring system lockdown”](#) on page 541.

About client installation methods

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

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

Table 5-5 Client installation options

Options	Description
Web Link and Email	<p>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.</p> <p>You can install Windows, Mac, and Linux clients using this option.</p> <p>See “Installing clients with Web Link and Email” on page 118.</p>
Remote Push	<p>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.</p> <p>You can install Windows and Mac clients using this option.</p> <p>See “Installing clients with Remote Push” on page 120.</p> <p>See “Preparing Windows and Mac computers for remote deployment” on page 111.</p>
Save Package	<p>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.</p> <p>You can install Windows, Mac, and Linux clients using this option.</p> <p>See “Installing clients with Save Package” on page 122.</p>

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 [“Which features should you install on the client?”](#) on page 117.

See [“About the Windows client installation settings”](#) on page 126.

See [“Preparing for client installation”](#) on page 108.

Which features should you 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 includes multiple protection components that 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.

[Table 5-6](#) lists the default feature sets for Windows clients and their roles.

Table 5-6 Client installation feature sets

Feature set	Description
Full Protection for Clients	<p>Recommended for workstations, desktop, and laptop computers.</p> <p>Includes all protection technologies. Appropriate for laptops, workstations, and desktops. Includes the full download protection and mail protocol protection.</p> <p>Note: Whenever possible, use Full Protection for maximum security.</p>
Full Protection for Servers	<p>Recommended for servers.</p> <p>Includes all protection technologies except email scanner protection. Appropriate for any servers that require maximum network security, including the Symantec Endpoint Protection Manager server.</p>
Basic Protection for Servers	<p>Recommended for high-throughput servers.</p> <p>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.</p>

After installation, you can enable or disable some features within of the protection components in the security policies.

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.

See [“How Symantec Endpoint Protection uses layers to protect computers”](#) on page 36.

See [“Configuring Windows client installation feature sets”](#) on page 127.

See [“About enabling and disabling protection when you need to troubleshoot problems”](#) on page 256.

See [“About client installation methods”](#) on page 115.

See [“Preparing for client installation”](#) on page 108.

Installing 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 628.

To install clients with Web Link and Email

- 1 In the console, on the **Home** page, in the **Common Tasks** menu, select **Install protection client to computers**.
- 2 In the **Client Deployment Wizard**, click **New Package Deployment**, 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 third-party security software on the Windows client, you must configure custom Client Install Settings before launching the Client Deployment Wizard. To see which third-party software the client package removes, see [About the third-party security software removal feature in Symantec Endpoint Protection 12.1](#).

See [“Configuring client packages to uninstall existing third-party security software”](#) on page 127.

See [“How Symantec Endpoint Protection uses layers to protect computers”](#) on page 36.

See [“About the Windows client installation settings”](#) on page 126.

- 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 129.

See [“Running a report on the deployment status of clients”](#) on page 600.

See [“Which features should you install on the client?”](#) on page 117.

See [“About client installation methods”](#) on page 115.

See [“Preparing for client installation”](#) on page 108.

Installing 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 knowledge base article:

[Installing the Bonjour Service for Symantec Endpoint Protection Manager 12.1.5 or later](#)

- 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 clients with Remote Push

- 1 In the console, on the **Home** page, in the **Common Tasks** menu, click **Install protection client to computers**.
- 2 In the **Client Deployment Wizard**, do one of the following tasks:
 - Click **New Package Deployment** to create a new installation package, and then click **Next**.
 - Click **Existing Package Deployment** to use a package that was previously created, and then click **Browse** to locate the package to install.
The Client Deployment Wizard uploads the package and directs you to the **Computer Selection** panel (step 5).
 - Click **Communication Update Package Deployment** if you want to update 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 175.
- 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**.

To uninstall third-party 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. To see which third-party software the client package removes, see [About the Security Software Removal feature in Symantec Endpoint Protection 12.1](#).

See [“About the Windows client installation settings”](#) on page 126.
- 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 129.

See [“Running a report on the deployment status of clients”](#) on page 600.

See [“Preparing for client installation”](#) on page 108.

See [“Preparing Windows and Mac computers for remote deployment”](#) on page 111.

See [“Which features should you install on the client?”](#) on page 117.

See [“About client installation methods”](#) on page 115.

Installing clients with Save Package

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.

Either you or the end user can install the installation package on the client computer. Alternately, you can use third-party deployment software to perform the installation.

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 clients with Save Package

- 1 In the console, on the **Home** page, in the **Common Tasks** menu, click **Install protection client to computers**.
- 2 In the **Client Deployment Wizard**, 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 third-party security software on the Windows client, you must configure custom Client Install Settings before launching the Client Deployment Wizard. To see which third-party software the client package removes, see [About the third-party security software removal feature in Symantec Endpoint Protection 12.1](#)

See [“Configuring client packages to uninstall existing third-party security software”](#) on page 127.

See [“About the Windows client installation settings”](#) on page 126.

- 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.

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

- 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 129.

See [“Running a report on the deployment status of clients”](#) on page 600.

See [“Which features should you install on the client?”](#) on page 117.

See [“About client installation methods”](#) on page 115.

See [“Preparing for client installation”](#) on page 108.

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 only need 32-bit or 64-bit installation packages for Windows, or only need `DPKG` or `RPM` installation packages for Linux. You also may need to create an unmanaged client with custom policies.

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 of installation package you export.

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

- 6 Click **OK**.

See [“Managing client installation packages”](#) on page 140.

See [“Installing clients with Save Package”](#) on page 122.

See [“Installing clients with Remote Push”](#) on page 120.

See [“Restoring client-server communications with Communication Update Package Deployment”](#) on page 175.

See [“Preparing for client installation”](#) on page 108.

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.

Note: 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 and Lotus Notes.

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 [“Which features should you install on the client?”](#) on page 117.

See [“Installing clients with Remote Push”](#) on page 120.

See [“How Symantec Endpoint Protection uses layers to protect computers”](#) on page 36.

See [“Preparing for client installation”](#) on page 108.

Configuring Windows client installation feature sets

Client installation feature sets define the client protection components that you install on Windows computers. For example, if you create Symantec Endpoint Protection packages you can select a feature set to only install Virus and Spyware Protection and Network Threat Protection.

You can also create and name a custom feature set. You then select a default or a custom client feature set when you export client software packages.

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

To configure a Windows client installation feature set

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

See [“Which features should you install on the client?”](#) on page 117.

See [“How Symantec Endpoint Protection uses layers to protect computers”](#) on page 36.

See [“Preparing for client installation”](#) on page 108.

Configuring client packages to uninstall existing third-party security software

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

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

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. See the documentation for the third-party software.

Note: You cannot remove third-party security software with Mac or Linux client packages. You also cannot configure installation packages for versions earlier than Symantec Endpoint Protection 12.1.1101 for Windows to remove third-party security software. You must uninstall third-party security software before you deploy the Symantec Endpoint Protection client package.

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

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

- 1 In the console, on the **Admin** page, click **Install Packages**, and then click **Client Install Settings**.
- 2 Under **Tasks**, click **Add Client Install Settings**.

Note: If you have previously created a custom client 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 **Automatically uninstall existing security software**, and then click **OK**.

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

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

- 1 On the **Home** page, in the **Common Tasks** drop-down list, click **Install protection client to computers**.
- 2 In the **Client Deployment Wizard**, click **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 [“About client installation methods”](#) on page 115.
- See [“About the Windows client installation settings”](#) on page 126.
- See [“Preparing for client installation”](#) on page 108.

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 126.

See [“About commands that you can run on client computers”](#) on page 258.

See [“Running commands on client computers from the console”](#) on page 261.

See [“Preparing for client installation”](#) on page 108.

Installing the Symantec Endpoint Protection client for Mac

You can directly install an unmanaged or managed 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 you create with 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 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 FileConnect, 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 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.

See [“Exporting client installation packages”](#) on page 124.

See [“Restoring client-server communications with Communication Update Package Deployment”](#) on page 175.

See [“Installing clients with Save Package”](#) on page 122.

See [“Installing clients with Remote Push”](#) on page 120.

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 179.

See [“Preparing for client installation”](#) on page 108.

About managed and unmanaged clients

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

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 5-7 Differences between a managed and an unmanaged client

Type	Description
Managed client	<p>You administer the clients from the console. Managed client computers connect to your network. You use the console to update the client software, security policies, and virus definitions on the managed client computers.</p> <p>In most cases, you install the client software as a managed client.</p> <p>You can install a managed client in one of the following ways:</p> <ul style="list-style-type: none">■ During initial product installation■ From the console after installation
Unmanaged client	<p>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.</p> <p>See “Download an unmanaged Symantec Endpoint Protection client installation package” on page 135.</p> <p>See “Installing an unmanaged Windows client” on page 136.</p>

See [“Why do I need to replace the client-server communications file on the client computer?”](#) on page 173.

See [“Preparing for client installation”](#) on page 108.

Download an unmanaged Symantec Endpoint Protection client installation package

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

- A standalone installer you download from FileConnect
[Download the latest version of Symantec Endpoint Protection](#)
- From within the installation file, whether you downloaded it from FileConnect, or received a physical disc

Note: The folder SEP contains the unmanaged Windows client, SEP_MAC contains the unmanaged Mac client, and SEP_LINUX contains the unmanaged Linux client.

- Exported an unmanaged client from Symantec Endpoint Protection Manager, with the default policies or with the policies from a group or groups

Note: 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 [“About managed and unmanaged clients”](#) on page 134.

See [“Exporting client installation packages”](#) on page 124.

Installing an unmanaged Windows client

You install an unmanaged Symantec Endpoint Protection client directly on to a Windows computer. This type of installation usually requires user input. However, you can export an unmanaged package through Symantec Endpoint Protection Manager with custom installation settings.

If you install a managed Windows client directly, only an **Interactive** installation requires user input. In this situation, the steps to install are similar to those of the unmanaged client. **Show progress bar only** or **Silent** installations do not require user input.

See [“Exporting client installation packages”](#) on page 124.

To install an unmanaged Windows client

- 1 Copy the installation file or 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 The installer selects **Unmanaged client** by default. Click **Next**. If you click **Managed client**, the installer advises you to install using a managed client installation package, and then quits.

This panel appears when you install the client software for the first time on a computer.
- 4 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 [“Which features should you install on the client?”](#) on page 117.
- 5 If the installation wizard prompts you, click **Enable Auto-Protect** and **Run LiveUpdate**, and then click **Next**
- 6 On the **File Reputation Data Submission** panel, uncheck the box if you do not want to provide anonymous 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 105.
- 7 On the **Ready to Install the Program** panel, click **Install**.
- 8 On the **Wizard Complete** panel, click **Finish**.

See [“Installing the Symantec Endpoint Protection client for Mac”](#) on page 130.
See [“Installing the Symantec Endpoint Protection client for Linux”](#) on page 132.
See [“About the Windows client installation settings”](#) on page 126.
See [“About managed and unmanaged clients”](#) on page 134.
See [“Preparing for client installation”](#) on page 108.

Uninstalling the Symantec Endpoint Protection client for Windows

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

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.

See your Windows documentation for more information.

To uninstall the Symantec Endpoint Protection client for Windows

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

- 1 On the client computer, on the **Start** menu, click **Control Panel > Add or Remove Programs** (or **Control Panel > Programs > Uninstall a program**).
- 2 In the **Add or Remove Programs** (or **Uninstall or change a program**) dialog box, click **Symantec Endpoint Protection**, and then click **Change, Remove** or **Uninstall**.
- 3 Follow the onscreen prompts to remove the client software.

See [“About client installation methods”](#) on page 115.

If the standard Windows uninstall method fails, you may have to uninstall the client manually. For more information, see the knowledge base article: [Uninstall Symantec Endpoint Protection](#).

Uninstalling the Symantec Endpoint Protection client for Mac

You uninstall the Symantec Endpoint Protection client for Mac with the Symantec Uninstaller that is included on the installation file in the `SEP_MAC` folder. The installation file may be one that you downloaded from FileConnect, or a physical disc.

Two files are provided in the `.tgz` archive file:

- `Symantec Uninstaller`, which is the actual uninstaller for the Symantec Endpoint Protection client for Mac.
- `SymantecUninstaller.pkg`, which lets you install the Symantec Uninstaller onto the client computer.

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

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

To uninstall the Symantec Endpoint Protection client for Mac

- 1 Copy the Symantec Uninstaller .tgz archive file to the Mac client computer.
- 2 Double-click the .tgz file to extract the Symantec Uninstaller folder using Archive Utility.
- 3 Double-click `Symantec Uninstaller`.
- 4 In the **Delete** column, check the box in front of Symantec Endpoint Protection, and then click **Uninstall**.
- 5 Click **Uninstall** again to confirm, and then authenticate with your Mac's administrative user name and password when prompted.
- 6 Click **Restart**.

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

For more information, see: [Uninstall Symantec Endpoint Protection](#).

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

You can export these packages as a single executable file or as a series of files in a directory. The method that you choose depends on your deployment method and whether you want to upgrade client software in groups. Typically, if you use Active Directory Group Policy Object, you do not choose to export to a single executable file.

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

Table 5-8 Client installation package-related tasks

Task	Description
Configure client installation packages	<p>You can select specific client protection technologies to install and you can specify how the installation interacts with end users.</p> <p>See “Configuring Windows client installation feature sets” on page 127.</p> <p>See “About the Windows client installation settings” on page 126.</p>
Export client installation packages	<p>You can export packages for managed clients or unmanaged clients. You can also export packages to install with third-party deployment tools.</p> <p>See “Exporting client installation packages” on page 124.</p>
Add client installation package updates	<p>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.</p> <p>See “Adding client installation package updates” on page 142.</p>
Upgrade Windows clients in one or more groups	<p>You can install the exported packages to computers one at a time, or deploy the exported files to multiple computers simultaneously.</p> <p>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 clients in groups with the latest software is to use AutoUpgrade. You should first update a group with a small number of test computers.</p> <p>See “Upgrading Windows clients by using AutoUpgrade in Symantec Endpoint Protection” on page 158.</p> <p>You can also update clients with LiveUpdate if you permit clients to run LiveUpdate and if the LiveUpdate Settings policy permits updates.</p>

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

Task	Description
Delete client installation packages	You can delete older client installation packages to save disk space. However, 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 108.

Adding client installation package updates

You can add a client installation package update to Symantec Endpoint Protection Manager. For example, you can add a newer client installation package to an existing Symantec Endpoint Protection Manager installation if you cannot immediately upgrade Symantec Endpoint Protection Manager.

You can optionally export the packages during this procedure for installation at a later time.

Note: An installation package that you import consists of two files. One file is named *product_name.dat*, and the other file is named *product_name.info*. These files automatically import during the installation or upgrade of Symantec Endpoint Protection Manager.

To add client installation package updates

- 1 Copy the package to a directory on the computer that runs Symantec Endpoint Protection Manager.
- 2 In the console, click **Admin**, and then click **Install Packages**.
- 3 Under **Tasks**, click **Add a Client Install Package**.
- 4 In the **Add a Client Install Package** dialog box, type a name and a description for the package.
- 5 Click **Browse**.
- 6 In the **Select Folder** dialog box, locate and select the *product_name.info* file for the new package, and then click **Select**.
- 7 When the **Completed successfully** prompt appears, do one of the following tasks:

- If you do not want to export the installation files and make them available for deployment, click **Close**.
You are finished with this procedure.
 - If you do want to export the installation files and make them available for deployment, click **Export this Package**, and then complete this procedure.
- 8 In the **Export Package** dialog box, click **Browse**.
 - 9 In the **Select Export Folder** dialog box, browse to and select the directory to contain the exported package, and then click **OK**.
 - 10 In the **Export Package** dialog box, select a group, and then set the other options according to your installation goals.
For details about setting other options in this dialog box, click **Help**.
 - 11 Click **OK**.
- See [“Managing client installation packages”](#) on page 140.
- See [“Preparing for client installation”](#) on page 108.

Upgrading Symantec Endpoint Protection

This chapter includes the following topics:

- [Upgrading to a new release](#)
- [Upgrade resources for Symantec Endpoint Protection 12.1.x](#)
- [Supported upgrade paths to Symantec Endpoint Protection](#)
- [Increasing Symantec Endpoint Protection Manager available disk space before upgrading to version 12.1.x](#)
- [Upgrading a management server](#)
- [Upgrading an environment that uses multiple embedded databases and management servers](#)
- [Turning off replication before an upgrade from Symantec Endpoint Protection 11.0](#)
- [Turning on replication after an upgrade from Symantec Endpoint Protection 11.0](#)
- [Stopping and starting the management server service](#)
- [About upgrading client software](#)
- [Upgrading Windows clients by using AutoUpgrade in Symantec Endpoint Protection](#)
- [Updating client software with a LiveUpdate Settings policy](#)
- [Upgrading Group Update Providers](#)
- [Enabling Symantec Network Access Control functionality in Symantec Endpoint Protection](#)

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 and System Requirements for all versions of Symantec Endpoint Protection and Symantec Network Access Control](#)
- New features in this version
See [“What's new in Symantec Endpoint Protection 12.1.6”](#) on page 30.
- Compatible Symantec Endpoint Protection Manager and Symantec Endpoint Protection client upgrade paths
See [“Supported upgrade paths to Symantec Endpoint Protection”](#) on page 148.

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.

Note: If you upgrade from 11.0, remove any packages that are assigned to the client groups. The **Maintain existing client features when upgrading** option on the 11.0 package causes the upgrade to remove all protection technologies from the clients.

For more information, see: [Clients show "No Symantec protection technologies are installed" after migrating the SEPM from 11.x to 12.1](#)

[Table 6-1](#) displays the steps you need to perform to upgrade to the latest version of Symantec Endpoint Protection.

Table 6-1 Process for upgrading to the Symantec Endpoint Protection enterprise version

Step	Action	Description
Step 1	Back up the database	Back up the database that Symantec Endpoint Protection Manager uses to ensure the integrity of your client information. See “Backing up the database and logs” on page 733.
Step 2	Turn off replication	If you upgrade from a Symantec Endpoint Protection 11.0 network, turn off replication on all sites that are configured as replication partners. Any attempts to replicate the database between Symantec Endpoint Protection versions during the upgrade corrupts the database. Symantec Endpoint Protection 12.1 and later does not allow replication if the product versions do not match. See “Turning off replication before an upgrade from Symantec Endpoint Protection 11.0” on page 155.
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 156.
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 152.
Step 5	Turn on replication after the upgrade	Turn on replication when the installation is complete to restore your configuration. See “Turning on replication after an upgrade from Symantec Endpoint Protection 11.0” on page 155.

Table 6-1 Process for upgrading to the Symantec Endpoint Protection enterprise version (*continued*)

Step	Action	Description
Step 6	Upgrade Symantec client software	<p>Prepare then upgrade your client software to the latest version. If you use Group Update Providers, they must be upgraded first.</p> <p>See “About upgrading client software” on page 157.</p> <p>See “Upgrading Group Update Providers” on page 161.</p> <p>See “Preparing for client installation” on page 108.</p> <p>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 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.</p> <p>See “Upgrading Windows clients by using AutoUpgrade in Symantec Endpoint Protection” on page 158.</p> <p>You can also update clients with LiveUpdate if you permit clients to run LiveUpdate and if the LiveUpdate Settings policy permits.</p> <p>See “Updating client software with a LiveUpdate Settings policy” on page 160.</p> <p>Note: If you upgrade from 11.0 and use Application and Device Control, you must disable the Application Control rule "Protect client files and registry keys." After the clients receive the new policy, you may upgrade the client computers.</p> <p>See “Creating a custom rule set and adding rules” on page 535.</p>

Upgrade resources for Symantec Endpoint Protection 12.1.x

[Table 6-2](#) provides the additional information to upgrade.

Table 6-2 Upgrade resources

Item	Resource
Client installation package settings and features	<p>You can configure client installation packages with a variety of settings and protection features.</p> <p>See “The types of security policies” on page 318.</p> <p>See “Client protection features based on platform” on page 775.</p> <p>See “About the Windows client installation settings” on page 126.</p> <p>See “Configuring Windows client installation feature sets” on page 127.</p>
Feature and policy descriptions	See “How Symantec Endpoint Protection uses layers to protect computers” on page 36.
Feature dependencies	See “How Symantec Endpoint Protection policy features work together on Windows computers” on page 437.
Manage product licenses	<p>Symantec Endpoint Protection 12.1 is licensed according to the number of clients that are needed to protect the computers at your site.</p> <p>See “Product license requirements” on page 61.</p> <p>See “About product upgrades and licenses” on page 100.</p>
Additional resources	See the knowledge base article: Best practices for upgrading to the latest version of Symantec Endpoint Protection 12.1.x

See [“Upgrading to a new release”](#) on page 145.

Supported upgrade paths to Symantec Endpoint Protection

Windows client and management server

The following Symantec Endpoint Protection Manager versions and Symantec Endpoint Protection Windows client versions can upgrade directly to 12.1.6:

- 11.0.x
- 12.0.122.192 Small Business Edition
- 12.0.1001.95 Small Business Edition - Release Update 1 (RU1)
- 12.1.671.4971 (RTM)
- 12.1.1000.157 - Release Update 1 (RU1)
- 12.1.1101.401 - Release Update 1, Maintenance Patch 1 (RU1 MP1)

- 12.1.2015.2015 - Release Update 2 (RU2)
- 12.1.2100.2093 - Release Update 2, Maintenance Patch 1 (RU2 MP1)
- 12.1.3001.165 - Release Update 3 (RU3)
- 12.1.4013.4013 - Release Update 4 (RU4)
- 12.1.4023.4080 - Release Update 4a (RU4a)
- 12.1.4100.4126 - Release Update 4, Maintenance Patch 1 (RU4 MP1)
- 12.1.4104.4130 - Release Update 4, Maintenance Patch 1a (RU4 MP1a)
- 12.1.4112.4156 - Release Update 4, Maintenance Patch 1b (RU4 MP1b)
- 12.1.5337.5000 - Release Update 5 (RU5)

Note: Symantec Endpoint Protection 12.1.6 does not ship with Small Business Edition, which reached end of life (EOL) in May, 2015. Small Business Edition 12.1 customers can use a tool to migrate to the cloud-based Symantec Endpoint Protection Small Business Edition. For more information, see:

[Migrating to Symantec Endpoint Protection Small Business Edition](#)

For details on upgrading from specific versions of Symantec Endpoint Protection Manager 11.0 to 12.1, see:

[Supported upgrade paths to Symantec Endpoint Protection Manager 12.1 from Symantec Endpoint Protection Manager 11.x](#)

Mac client

The following Symantec Endpoint Protection client for Mac versions can upgrade directly to 12.1.6:

- 11.0.x
- 12.1.671.4971 (RTM)
- 12.1.1000.0157 - Release Update 1 (RU1)
- 12.1.2015.2015 - Release Update 2 (RU2)
- 12.1.4013.4013 - Release Update 4 (RU4)
- 12.1.5337.5000 - Release Update 5 (RU5)

Note: The Symantec Endpoint Protection client for Mac did not update for Release Update 3 (RU3).

Linux client

The following Symantec Endpoint Protection client for Linux version can upgrade directly to 12.1.6:

- 12.1.5337.5000 - Release Update 5 (RU5)

You can only migrate Symantec AntiVirus for Linux 1.0.14 directly to Symantec Endpoint Protection for Linux. 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 12.1.6 client:

- The legacy Symantec products Symantec AntiVirus and Symantec Client Security
- All Symantec Norton products
- Symantec Endpoint Protection for Windows XP Embedded 5.1

Downgrade paths are not supported, such as migrating from Symantec Endpoint Protection 12.1.x to 11.x, or Symantec Endpoint Protection for Linux to Symantec AntiVirus to Linux. In these cases, you must uninstall the older product or earlier version of the product first.

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

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.

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

See [“Backing up the database and logs”](#) on page 733.

[Table 6-3](#) lists ways you can make more disk space available for the upgrade.

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

Table 6-3 Tasks to increase disk space on the management server

Task	Description
<p>Change the LiveUpdate settings to reduce space requirements.</p>	<ol style="list-style-type: none"> <li data-bbox="454 326 1217 383">1 Go to Admin > Servers and right-click Local Site. Select Edit Site Properties. <li data-bbox="454 395 1217 552">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. <li data-bbox="454 574 1217 951">3 On the LiveUpdate tab, reduce the number of content revisions to keep. The optimum value is 30 revisions but a lower setting uses less disk space. For the upgrade, you can lower the setting to 10. Allow time for Symantec Endpoint Protection Manager to purge the extra revisions. 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. If you upgrade from a version earlier than 12.1.5, 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 “Managing content updates” on page 181. See “Configuring a site to download content updates” on page 189.
<p>Make sure that unused virus definitions are deleted from the Symantec Endpoint Protection Manager database.</p>	<ol style="list-style-type: none"> <li data-bbox="454 1085 1217 1241">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. <li data-bbox="454 1263 1217 1310">2 On the Log Settings tab, under Risk Log Settings, make sure that Delete unused virus definitions is checked.

Table 6-3 Tasks to increase disk space on the management server (*continued*)

Task	Description
Relocate or remove co-existing programs and files	<ul style="list-style-type: none"> ■ 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 knowledge base article, Symantec Endpoint Protection Manager directories contain many .TMP folders consuming large amounts of disk space. <p>Note: Defragment the hard drive after removing programs and files.</p>
Use an external database	<p>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.</p> <p>See “About choosing a database type” on page 65.</p>

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.

[Low Disk Space issues encountered on systems running either the Symantec Endpoint Protection client or the Symantec Endpoint Protection Manager](#)

[Low disk space on a Symantec Endpoint Protection client](#)

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

Upgrading a management server

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

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

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

The upgrade process is similar to a fresh installation.

[Table 6-4](#) lists the tasks to upgrade Symantec Endpoint Protection Manager.

Table 6-4 Upgrade tasks

Task	Description
Upgrade the management server	<p>Upgrade the management server, and then configure it with the Management Server Configuration Wizard.</p> <p>Note: You may need to edit the security policies to allow the virtual service accounts to run correctly for Windows 7 / Server 2008 R2 or later. Earlier operating systems are not affected, but require Network Service to be present in security policies.</p> <p>As of 12.1.6, the Symantec Endpoint Protection Manager upgrade automatically changes local security policies to grant the correct user rights to Symantec Endpoint Protection Manager virtual service accounts. If domain policies do not comply with the required user rights, a warning appears with more information and identifies which domain policies you must change. A warning also appears if the domain policies cannot be read.</p> <p>For more information, see:</p> <p>How to assign user rights to the Windows Security Policies for Symantec Endpoint Protection Manager services</p> <p>See “Installing Symantec Endpoint Protection Manager” on page 74.</p> <p>See “Upgrading an environment that uses multiple embedded databases and management servers” on page 154.</p>
Log onto the management server	<p>When the Symantec Endpoint Protection Manager logon panel appears, you can log on to the console by using your logon credentials.</p> <p>See “Logging on to the Symantec Endpoint Protection Manager console” on page 78.</p>

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 712.

See [“Setting up sites and replication”](#) on page 718.

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 On all management servers, disable replication.

This step is required for upgrades from Symantec Endpoint Protection Manager 11.0, because attempts to replicate during the upgrade process corrupt the database due to a product version mismatch. Symantec Endpoint Protection Manager 12.1 and later does not allow replication if the product versions do not match.

See [“Turning off replication before an upgrade from Symantec Endpoint Protection 11.0”](#) on page 155.

- 2 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.

- 3 Upgrade the management server.

See [“Upgrading a management server”](#) on page 152.

- 4 Upgrade all additional management servers one by one.

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

See [“Turning on replication after an upgrade from Symantec Endpoint Protection 11.0”](#) on page 155.

Turning off replication before an upgrade from Symantec Endpoint Protection 11.0

If you have a legacy Symantec Endpoint Protection 11.0 site in which you use replication, you must turn off replication before you upgrade. Due to a database schema mismatch, the replication of data between legacy and updated databases during or after the upgrade corrupts the database. You must turn off replication at each site that replicates. You must log on to and turn off replication at a minimum of two sites.

Symantec Endpoint Protection 12.1 and later does not require that you turn off replication before you upgrade. Symantec Endpoint Protection 12.1 and later does not allow replication if the database schema versions do not match.

See [“Turning on replication after an upgrade from Symantec Endpoint Protection 11.0”](#) on page 155.

To turn off replication before an upgrade from Symantec Endpoint Protection 11.0

- 1 In the console, click **Admin > Servers**.
- 2 Under **Servers**, expand **Replication Partners** and select a site.
- 3 Right-click the site, and then click **Delete**.
- 4 Click **Yes**.
- 5 Log off the console, and then repeat this procedure at all sites that replicate data.

Turning on replication after an upgrade from Symantec Endpoint Protection 11.0

After you upgrade the Symantec Endpoint Protection 11.0 servers that used replication, you must turn on replication again to use it. To turn on replication, you add the replication partner or partners on the computer on which you first installed the management server. Replication partners automatically appear on the other management servers.

See [“Turning off replication before an upgrade from Symantec Endpoint Protection 11.0”](#) on page 155.

See [“Upgrading to a new release”](#) on page 145.

To turn on replication after an upgrade from Symantec Endpoint Protection 11.0

- 1 On the console, click **Admin > Servers**.
- 2 Under **Servers**, expand **Replication Partners** and select a site.

- 3 Right-click the site, and then click **Add Partner**.
- 4 In the **Add Replication Partner** panel, click **Next**.
- 5 In the **Remote Site Information** panel, enter the identifying information about the replication partner, enter the authentication information, and then click **Next**.
- 6 In the **Schedule Replication** panel, set the schedule for when replication occurs automatically, and then click **Next**.
- 7 In the **Replication of Log Files and Client Packages** panel, check the items to replicate, and then click **Next**.
Package replication uses large amounts of traffic and hard disk space.
- 8 In the **Completing the Add Replication Partner Wizard** panel, click **Finish**.
- 9 Repeat this procedure for all computers that replicate data with this computer.

Stopping and starting the management server service

Before you upgrade from Symantec Endpoint Protection 11.0, you must manually stop the Symantec Endpoint Protection Manager service on every management server in your site. After you upgrade, the service starts automatically.

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

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

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

See [“Upgrading to a new release”](#) on page 145.

To stop the Symantec Endpoint Protection Manager service

- 1 Click **Start > Settings > Control Panel > Administrative Tools > Services**.
- 2 In the **Services** window, under **Name**, scroll to and right-click **Symantec Endpoint Protection Manager**.
- 3 Click **Stop**.

- 4 Close the Services window.

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

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

Note: To start the Symantec Endpoint Protection Manager service, follow the above procedure and click **Start** instead of **Stop**.

To stop the Symantec Endpoint Protection Manager service using the command line

- ◆ From a command prompt, type:

```
net stop semsrv
```

To start the Symantec Endpoint Protection Manager service using the command line

- ◆ From a command prompt, type:

```
net start semsrv
```

About upgrading client software

You can use several methods to upgrade Symantec client software. Some methods can take up to 30 minutes. Therefore, you may want to upgrade client software when most users are not logged on to their computers.

Table 6-5 Methods to upgrade the client software

Upgrade method	Description
AutoUpgrade	Use AutoUpgrade to update Windows clients in one or more groups from the Symantec Endpoint Protection Manager console. See “Upgrading Windows clients by using AutoUpgrade in Symantec Endpoint Protection” on page 158.

Table 6-5 Methods to upgrade the client software (*continued*)

Upgrade method	Description
LiveUpdate Settings policy	<p>Configure a LiveUpdate Settings policy for a group that defines a LiveUpdate server and allows clients to run LiveUpdate to obtain product updates.</p> <p>See “Updating client software with a LiveUpdate Settings policy” on page 160.</p>
Installation file	<p>Use the installation file you download from FileConnect to install a new version of the client.</p>
Other methods	<p>Use one of the other supported methods of installing client software.</p> <p>See “About client installation methods” on page 115.</p>

See [“Upgrading to a new release”](#) on page 145.

Upgrading Windows clients by using AutoUpgrade in Symantec Endpoint Protection

The AutoUpgrade process lets you automatically upgrade the Symantec Endpoint Protection client software for all the Windows clients that are contained in a group. For example, you can use AutoUpgrade to upgrade clients to a new release update or product version.

With AutoUpgrade, standard-size clients receive a delta upgrade package that Symantec Endpoint Protection Manager creates. This package is smaller than the full installation package. Reduced-size clients always receive the full installation package, since these clients do not maintain a copy of the installer in the installer cache.

Use the following best practices for using AutoUpgrade:

- You must test the AutoUpgrade process before you attempt to upgrade a large number of clients in your production network. If you do not have a test network, you can create a test group within your production network. For this kind of test, you add a few non-critical clients to the test group and then upgrade them by using AutoUpgrade.
- If you upgrade from 11.0 and use Application and Device Control, you must disable the Application Control rule **Protect client files and registry keys**. After the clients receive the new policy, you may upgrade using AutoUpgrade. See [“Creating a custom rule set and adding rules”](#) on page 535.

- 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.

You confirm that the upgrade completed successfully by verifying the version number of the client software. The version number is displayed in the client's **Help > About** panel. The updated client version number is also displayed in Symantec Endpoint Protection Manager on the **Clients** page after a successful check-in. You click the group, then the **Clients** tab, and change the view to **Client Status**.

See [“About upgrading client software”](#) on page 157.

To upgrade Windows clients by using AutoUpgrade in Symantec Endpoint Protection

- 1 In the Symantec Endpoint Protection Manager console, click **Admin**.
- 2 Click **Install Packages**.
- 3 Under **Tasks**, click **Upgrade Clients with Package**.
- 4 In the **Upgrade Clients Wizard** panel, click **Next**.
- 5 In the **Select Client Install Package** panel, select the appropriate client installation package, and then click **Next**.
- 6 In the **Specify Groups** panel, select the groups that contain the client computers that you want to upgrade, and then click **Next**.
- 7 In the **Package Upgrade Settings** panel, select **Download from the management server**.

To reduce bandwidth, stage and select a package on a web server that is local to the computers you upgrade.
- 8 Click **Upgrade Settings**.
- 9 On the **General** tab, select **Maintain existing client features when updating**.

You can optionally add or remove features when upgrading.
- 10 Optionally, on the **Notification** tab, customize the user notification settings. You can customize the message that is displayed on the client computer during the upgrade. You can also allow the user to postpone the upgrade by an amount of time you specify.

For more information about schedule and notification settings, click **Help**.
- 11 Click **OK**.
- 12 In the **Upgrade Clients Wizard Complete** panel, click **Next**.
- 13 Click **Finish**.

Updating client software with a LiveUpdate Settings policy

You can update Symantec Windows and Mac client product software automatically by permitting product updates with a LiveUpdate Settings policy. When product updates are permitted and an update is available, clients download and install them when a LiveUpdate session runs. You can schedule a LiveUpdate session or you can manually start it. When the LiveUpdate policy is not configured to download product updates, client software can be only updated by using the Symantec Endpoint Protection Manager console or manually.

By default, LiveUpdate for Symantec Endpoint Protection Manager downloads and processes client updates and patches. When the management server downloads a new client version, you can select the new package and upgrade clients with AutoUpgrade or with another upgrade method. You can disable this setting under **Admin > Local Site > Edit Site Properties > LiveUpdate**, under **Content Types to Download**.

You cannot update the Linux client product software with LiveUpdate.

See [“About upgrading client software”](#) on page 157.

See [“Upgrading Windows clients by using AutoUpgrade in Symantec Endpoint Protection”](#) on page 158.

See [“Managing content updates”](#) on page 181.

To update Symantec client software with a LiveUpdate Settings policy

- 1 In the Symantec Endpoint Protection Manager console, click **Policies > LiveUpdate**.
- 2 In the right pane, on the **LiveUpdate Settings** tab, click a LiveUpdate policy.
- 3 In the lower portion of the left pane, under **Tasks**, click **Edit the Policy**.
- 4 Under **Windows Settings**, click **Advanced Settings**, and then check **Download Symantec Endpoint Protection product updates using a LiveUpdate server**.
- 5 Under **Mac Settings**, click **Advanced Settings**, and then check **Download Symantec Endpoint Protection product updates using a LiveUpdate server**.
- 6 Click **OK**, and then apply the policy to a group or a location in a group.

See [“Performing the tasks that are common to all policies”](#) on page 315.

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 145.

Enabling Symantec Network Access Control functionality in Symantec Endpoint Protection

All versions of Symantec Endpoint Protection Manager include all of the Symantec Network Access Control features. As of version 12.1.6, Symantec does not provide a separate installation file for Symantec Network Access Control that you can download from FileConnect. Instead, you first install the management server and then enable the Symantec Network Access Control functionality on the management server.

Before you start, you need the following items:

- The `snac.xml` file that is located in the `SNAC_12.1.6_XML_Multi.zip` file on FileConnect:
<https://fileconnect.symantec.com>
- Access to the computer on which the management server runs.
- A Symantec Network Access Control license file (*.sfl) or a Symantec Network Access Control serial number.

To enable the Symantec Network Access Control functionality, do the following tasks:

1. Install Symantec Endpoint Protection Manager.

If you had previously installed Symantec Endpoint Protection and Symantec Network Access Control and upgrade to the latest version of Symantec Endpoint Protection Manager, the Symantec Network Access Control functionality appears automatically. If you have not already updated the management server to the most current version, upgrade the management server first.

[Installing Symantec Endpoint Protection Manager](#)

[Upgrading to a new release](#)

2. Copy the `snac.xml` file to the computer on which the management server runs and enable the Symantec Network Access Control functionality.

See “[Enabling Symantec Network Access Control in Symantec Endpoint Protection Manager](#)” on page 162.

3. Import your Symantec Network Access Control license or serial number into the Symantec Endpoint Protection Manager console.

[Activating or importing your Symantec Endpoint Protection 12.1.x product license](#)

Enabling Symantec Network Access Control in Symantec Endpoint Protection Manager

To upgrade Symantec Endpoint Protection with the Symantec Network Access Control functionality, you must first add the Symantec Network Access Control module to Symantec Endpoint Protection Manager. You must have both a license to run Symantec Network Access Control and the `snac.xml` file.

See “[Enabling Symantec Network Access Control functionality in Symantec Endpoint Protection](#)” on page 161.

To add the Symantec Network Access Control module to Symantec Endpoint Protection Manager

- 1 On the computer hosting Symantec Endpoint Protection Manager, click **Start** > **Run**, and then type `services.msc`.

- 2 In the **Services** dialog box, stop the following services:

Symantec Endpoint Protection Manager

Symantec Endpoint Protection Manager Webserver

- 3 Copy `snac.xml` to the following default folder:

For 32-bit: `C:\Program Files\Symantec\Symantec Endpoint Protection Manager\tomcat\etc\license`

For 64-bit: `C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\tomcat\etc\license`

- 4 Restart the Symantec Endpoint Protection Manager services.

To enable Symantec Network Access Control in Symantec Endpoint Protection Manager

- 1 In Symantec Endpoint Protection Manager, click **Clients**, and select the group for which you want to enable Symantec Network Access Control.

By default, Symantec Network Access Control is disabled for all clients.

- 2 On the **Policy** tab, click **General Settings** > **Security Settings** tab, and check **Enable Network Access Control**.

- 3 Restart the client computer.

To verify that Symantec Network Access Control is enabled on the client

- 1 On a Symantec Endpoint Protection client computer, right-click the Symantec Endpoint Protection shield icon in the notification area, and click **Update Policy**.
- 2 Open the client.
- 3 On the client **Status** page, **Network Access Control** appears.

[How to remove the Symantec Network Access Control module from both Symantec Endpoint Protection Manager and client](#)

Managing client-server communication and updating content

- [Chapter 7. Managing client-server communication](#)
- [Chapter 8. Updating content on the clients](#)

Managing client-server communication

This chapter includes the following topics:

- [Managing the client-server connection](#)
- [How to determine whether the client is connected in the console](#)
- [How to determine whether the client computer is connected and protected](#)
- [How the client computer and the management server communicate](#)
- [Configuring push mode or pull mode to update client policies and content](#)
- [Using the policy serial number to check client-server communication](#)
- [Why do I need to replace the client-server communications file on the client computer?](#)
- [How do I replace the client-server communications file on the client computer?](#)
- [Restoring client-server communications with Communication Update Package Deployment](#)
- [Exporting the client-server communications file \(Sylink.xml\) manually](#)
- [Importing client-server communication settings into the Windows client](#)
- [Importing client-server communication settings into the Linux client](#)

Managing the client-server connection

After you install the client, the management server automatically connects to the client computer. You may need to verify whether the client and server communicate.

You may also want to configure the connection between the server and client.

Table 7-1 lists the tasks you can perform to view and manage how the management server connects to clients.

Table 7-1 Tasks to manage connections between the management server and the clients

Action	Description
<p>Check whether the client is connected to the management server</p>	<p>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.</p> <p>See “How to determine whether the client is connected in the console” on page 167.</p> <p>A computer may have the client software installed, but does not have the correct communications file.</p> <p>See “Why do I need to replace the client-server communications file on the client computer?” on page 173.</p> <p>See “How do I replace the client-server communications file on the client computer?” on page 174.</p>
<p>Check that the client gets policy updates</p>	<p>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.</p> <p>You can perform a manual policy update and then check the policy serial numbers against each other.</p> <p>See “Using the policy serial number to check client-server communication” on page 172.</p> <p>See “Manually updating policies on the client” on page 315.</p>
<p>Change which method you use to download policies and content to the clients</p>	<p>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.</p> <p>See “Configuring push mode or pull mode to update client policies and content” on page 170.</p>
<p>Decide whether to use the default management server list</p>	<p>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.</p> <p>See “Configuring a management server list for load balancing” on page 715.</p>
<p>Configure communication settings for a location</p>	<p>You can configure separate communication settings for locations and for groups.</p> <p>See “Configuring communication settings for a location” on page 285.</p>

Table 7-1 Tasks to manage connections between the management server and the clients (*continued*)

Action	Description
Troubleshoot management server connectivity problems	<p>If the management server and the client do not connect, you can troubleshoot connection problems.</p> <p>See “Troubleshooting communication problems between the management server and the client” on page 745.</p>

For more information on the ports that Symantec Endpoint Protection uses, see the knowledge base article: [Which Communications Ports does Symantec Endpoint Protection use?](#)

How to determine whether the client is connected in the console

In Symantec Endpoint Protection Manager, you can use the client status icons to check whether the client and the server communicate.

Table 7-2 Client status icons in the management console

Icon	Description
	The client software installation failed.
	<ul style="list-style-type: none"> The client can communicate with Symantec Endpoint Protection Manager. The client is in computer mode.
	<ul style="list-style-type: none"> The client cannot communicate with Symantec Endpoint Protection Manager. The client is in computer mode. The client may have been added from the console, and may not have any Symantec client software installed.
	<ul style="list-style-type: none"> The client can communicate with Symantec Endpoint Protection Manager. The client is in computer mode. The client is an unmanaged detector.

Table 7-2 Client status icons in the management console (*continued*)

Icon	Description
	<ul style="list-style-type: none"> ■ The client cannot communicate with Symantec Endpoint Protection Manager. ■ The client is in computer mode. ■ The client is an unmanaged detector.
	<ul style="list-style-type: none"> ■ The client can communicate with Symantec Endpoint Protection Manager. ■ The client is in user mode.
	<ul style="list-style-type: none"> ■ 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.
	<ul style="list-style-type: none"> ■ The client can communicate with Symantec Endpoint Protection Manager at another site. ■ The client is in computer mode.
	<ul style="list-style-type: none"> ■ The client can communicate with Symantec Endpoint Protection Manager at another site. ■ The client is in computer mode. ■ The client is an unmanaged detector.
	<ul style="list-style-type: none"> ■ The client can communicate with Symantec Endpoint Protection Manager at another site. ■ The client is in user mode.

See [“Viewing the protection status of clients and client computers”](#) on page 253.

You can also look on the client to see whether or not it is connected to the management server.

See [“How to determine whether the client computer is connected and protected”](#) on page 169.

How to determine whether the client computer is connected and protected

You can check the notification area icon on the client to determine whether the client is connected to a management server and adequately protected. The notification area icon is sometimes referred to as the system tray.

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 7-3 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. For example, Network Threat Protection may be disabled.

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

See [“How to determine whether the client is connected in the console”](#) on page 167.

See [“Running a report on the deployment status of clients”](#) on page 600.

See [“Managing the client-server connection”](#) on page 165.

How the client computer and the management server communicate

When you configure policies on the management server, you need to have the updated policies downloaded to the client computers. In the console, you can configure client computers to use either of the following update methods:

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

In either mode, the client computer takes the corresponding action, based on the change in the status of the management server. Because it requires a constant connection, push mode requires a large amount of network bandwidth. Client computers that are configured to use pull mode require less bandwidth.

See [“Configuring push mode or pull mode to update client policies and content”](#) on page 170.

The heartbeat protocol defines the frequency at which client computers upload data such as log entries and download policies. The first heartbeat occurs immediately after the client starts. The next heartbeat occurs at the heartbeat frequency that you set.

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

Note: You can also update policies manually on a client computer.

See [“Using the policy serial number to check client-server communication”](#) on page 172.

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

You can specify whether Symantec Endpoint Protection Manager pushes the policy down to the clients or that the clients pull the policy from Symantec Endpoint

Protection Manager. The default setting is push mode. If you select pull mode, then by default, clients connect to the management server every 5 minutes, but you can change this default heartbeat interval.

See [“How the client computer and the management server communicate”](#) on page 169.

See [“Performing the tasks that are common to all policies”](#) on page 315.

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

Note: Windows XP supports a limited number of concurrent users if the clients are in push mode. It is a best practice to use pull mode when you deploy policies to up to 100 clients.

To configure push mode or pull mode for a group

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

To specify push mode or pull mode for a location

- 1 In the console, click **Clients**.
- 2 Under **Clients**, select the group for which you want to specify whether to push or pull policies.
- 3 Click **Policies**.
- 4 Uncheck **Inherit policies and setting from the parent group "group name"**.

- 5 Under **Location-specific Policies and Settings**, under **Location-specific Policies** for the location you want to modify, expand **Location-specific Settings**.
- 6 Under **Location-specific Settings**, to the right of **Communications Settings**, click **Tasks** and uncheck **Use Group Communications Settings**.
- 7 To the right of **Communications Settings**, click **Local - Push** or **(Local - Pull)**.
- 8 Do one of the following tasks:
 - Click **Push mode**.
 - Click **Pull mode** and under **Heartbeat Interval**, set the number of minutes or hours.
- 9 Click **OK**.

See [“Performing the tasks that are common to all policies”](#) on page 315.

Using the policy serial number to check client-server communication

To check whether the server and client communicate, check the policy serial number on the console and on the client. If the client communicates with the management server and receives regular policy updates, the serial numbers should match.

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

See [“Manually updating policies on the client”](#) on page 315.

See [“How the client computer and the management server communicate”](#) on page 169.

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.

Why do I need to replace the client-server communications file on the client computer?

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 315.

Why do I need to replace the client-server communications file on the client computer?

Symantec Endpoint Protection Manager connects to the client with a communications file called Sylink.xml. The Sylink.xml file includes the communication settings such as the IP address of the management server and the heartbeat interval. After you install a client installation package on to the client computers, the client and the server automatically communicate.

Normally you do not need to replace the Sylink.xml file. However, you may need to replace the existing Sylink.xml file on the client computer in the following situations:

- The client and the server do not communicate. If the clients have lost the communication with the management server, you must replace the old Sylink.xml file with a new file.
See [“Managing the client-server connection”](#) on page 165.
See [“Checking the connection to the management server on the client computer”](#) on page 747.
- 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 134.
- You want to manage a previously orphaned client. For example, if the hard drive that the management server is installed on gets corrupted, you must reinstall the management server. You can update the Sylink.xml file to re-establish communication with all your orphaned clients.
See [“Disabling or enabling secure communications between the server and the client”](#) on page 689.
- 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

How do I replace the client-server communications file on the client computer?

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 248.

- To install a Security Virtual Appliance in a VMware vShield environment. To install a Security Virtual Appliance, you must export the communications file manually.
See [“What do I need to do to install a Security Virtual Appliance?”](#) on page 654.
See [“Exporting the client-server communications file \(Sylink.xml\) manually”](#) on page 176.

See [“How do I replace the client-server communications file on the client computer?”](#) on page 174.

See [“Restoring client-server communications with Communication Update Package Deployment”](#) on page 175.

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 175.
- 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 752.
- 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 7-4 displays the process for exporting and importing the Sylink.xml file into the client computer.

Table 7-4 Steps for exporting and importing the communications file

Step	Task	Description
Step 1	Export a file that includes all the communication settings for the group that you want the client to be in.	The default file name is <i>group name_sylink.xml</i> . See “Exporting the client-server communications file (Sylink.xml) manually” on page 176.
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 178. Unmanaged clients are not password-protected, so you do not need a password on the client. However, if you try to import a file into a managed client that is password-protected, then you must enter a password. The password is the same one that is used to import or export a policy. See “Password-protecting the client” on page 273. You do not need to restart the client computer.
Step 4	Verify client and server communication on the client.	The client immediately connects to the management server. The management server places the client in the group that is specified in the communication file. The client is updated with the group's policies and settings. After the client and the management server communicate, the notification area icon with the green dot appears in the client computer's taskbar. See “How to determine whether the client is connected in the console” on page 167.

See [“Client and server communication files”](#) on page 757.

See [“Why do I need to replace the client-server communications file on the client computer?”](#) on page 173.

Restoring client-server communications with Communication Update Package Deployment

If the client-server communications breaks, you can quickly restore communications by replacing the Sylink.xml file on the client computer. You can replace the sylink.xml

file by redeploying a client installation package. Use this method for a large number of computers, for the computers that you cannot physically access easily, or the computers that require administrative access.

See [“Why do I need to replace the client-server communications file on the client computer?”](#) on page 173.

To restore client-server communication settings with Communication Update Package Deployment

- 1 On the **Home** page, in the **Common Tasks** drop-down list, click **Install protection client to computers**.
- 2 In the **Client Deployment Wizard**, click **Communication Update Package Deployment**, and then click **Next**.
- 3 Select from the following options, and then click **Next**.
 - The group of computers on which you want to deploy the client installation package.
 - The policy mode that applies to the protected computer.
 - The password to stop the client service, or import or export a policy, if you previously set one.
See [“Password-protecting the client”](#) on page 273.
- 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 clients with Remote Push”](#) on page 120.
 - **Save Package** and go to the **Browse** step in the following procedure.
See [“Installing clients with Save Package”](#) on page 122.
- 5 Confirm that the computer users installed the custom installation package.
You or the computer users must restart the client computers.
See [“Running a report on the deployment status of clients”](#) on page 600.
See [“Restarting the client computers from Symantec Endpoint Protection Manager”](#) on page 129.

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 [“Disabling or enabling secure communications between the server and the client”](#) on page 689.
- To install a Security Virtual Appliance in a VMware vShield environment.
 See [“What do I need to do to install a Security Virtual Appliance?”](#) on page 654.

See [“Why do I need to replace the client-server communications file on the client computer?”](#) on page 173.

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 175.

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**, select one of the following options:
 - To apply the policies from the group from which the computer is a member, click **Computer Mode**.
 - To apply the policies from the group from which the user is a member, click **User Mode**.

Note: Computer mode and user mode apply only to Windows client computers.

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 178.

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 with appears in the computer's taskbar. The green dot indicates that the client and the management server are in communication with each other.

See [“Exporting the client-server communications file \(Sylink.xml\) manually”](#) on page 176.

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.

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 176.

- 2 On the Linux computer, open a terminal window and enter the following command:

```
sudo ./sav manage -i path-to/sylink.xml
```

Where *path-to* represents the path to which you copied `sylink.xml`.

For example, if you copied it to your user profile's desktop, enter:

```
sudo ./sav manage -i ~/Desktop/sylink.xml
```

- 3 A successful import returns OK. To further verify the managed status, enter the followed command, which displays the policy serial number for a successful import:

```
./sav manage -p
```

See [“Installing the Symantec Endpoint Protection client for Linux”](#) on page 132.

Updating content on the clients

This chapter includes the following topics:

- [Managing content updates](#)
- [Configuring a site to download content updates](#)
- [Configuring the LiveUpdate download schedule for Symantec Endpoint Protection Manager](#)
- [Running LiveUpdate and downloading content to Symantec Endpoint Protection Manager immediately](#)
- [Mitigating network overloads for client update requests](#)
- [Checking LiveUpdate server activity](#)
- [Configuring Symantec Endpoint Protection Manager to connect to a proxy server to access the Internet and download content from Symantec LiveUpdate](#)
- [Specifying a proxy server that clients use to communicate to Symantec LiveUpdate or an internal LiveUpdate server](#)
- [Configuring the types of content used to update client computers](#)
- [Configuring the LiveUpdate download schedule for client computers](#)
- [Configuring the amount of control that users have over LiveUpdate](#)
- [Configuring the content revisions that clients use](#)
- [About randomization of simultaneous content downloads](#)
- [Randomizing content downloads from the default management server or a Group Update Provider](#)

- [Randomizing content downloads from a LiveUpdate server](#)
- [Configuring client updates to run when client computers are idle](#)
- [Configuring client updates to run when definitions are old or the computer has been disconnected](#)
- [Setting up an external LiveUpdate server for Symantec Endpoint Protection clients](#)
- [Setting up an internal LiveUpdate server for Symantec Endpoint Protection clients](#)
- [Using Group Update Providers to distribute content to clients](#)
- [Using Intelligent Updater files to update content on Windows computers](#)
- [Using third-party distribution tools to update client computers](#)

Managing content updates

By default, the Symantec Endpoint Protection Manager downloads content updates from the public Symantec LiveUpdate servers for Symantec Endpoint Protection clients. Symantec Endpoint Protection Windows 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 8-1 Tasks for managing content updates

Task	Description
Make sure that the management server has the latest content from LiveUpdate (Recommended)	<p>By default, LiveUpdate runs as part of the Symantec Endpoint Protection Manager installation. You may need to run LiveUpdate manually in the following situations:</p> <ul style="list-style-type: none"> ■ 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. <p>See “Running LiveUpdate and downloading content to Symantec Endpoint Protection Manager immediately” on page 193.</p>
Reduce network overloads (Recommended)	<p>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.</p> <p>See “Mitigating network overloads for client update requests” on page 193.</p>

Table 8-1 Tasks for managing content updates (*continued*)

Task	Description
Improve performance (Recommended)	<p>To help mitigate the effect of downloads on network bandwidth, download content randomly so that not all clients get updates at the same time.</p> <p>See “About randomization of simultaneous content downloads” on page 206.</p> <p>See “Randomizing content downloads from the default management server or a Group Update Provider” on page 207.</p> <p>See “Randomizing content downloads from a LiveUpdate server” on page 208.</p> <p>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.</p> <p>See “Configuring client updates to run when client computers are idle” on page 209.</p>
Change how client computers get updates (Optional)	<p>By default, Windows client computers get content updates from the management server. You may need to change the delivery method to support different client platforms, large numbers of clients, or network limitations.</p> <p>See “Choose a distribution method to update content on clients” on page 182.</p> <p>See “Choose a distribution method to update content on clients based on the platform” on page 187.</p>
Change the LiveUpdate settings for the management server (Optional)	<p>You can customize the frequency of LiveUpdate sessions, the protection components that are downloaded, and more.</p> <p>See “Configuring a site to download content updates” on page 189.</p> <p>See “Configuring the LiveUpdate download schedule for Symantec Endpoint Protection Manager” on page 192.</p>
Let your endpoint users manage their own updates (Optional)	<p>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.</p> <p>See “Configuring the amount of control that users have over LiveUpdate” on page 204.</p>

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.

See [“Choose a distribution method to update content on clients based on the platform”](#) on page 187.

See [“Managing content updates”](#) on page 181.

Table 8-2 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)	<p>The default management server automatically updates the client computers that it manages.</p> <p>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.</p> <p>You can change the download schedule from the LiveUpdate server to the management server.</p> <p>See “Configuring the LiveUpdate download schedule for Symantec Endpoint Protection Manager” on page 192.</p> <p>See “Configuring the LiveUpdate download schedule for client computers” on page 202.</p> <p>See “Configuring push mode or pull mode to update client policies and content” on page 170.</p>	<p>Symantec recommends that you use this method unless network constraints or your company's policies require an alternative.</p> <p>If you have a large number of clients or bandwidth issues, you might use this method, along with Group Update Providers.</p> <p>For Mac or Linux computers to receive content updates from the management server, you must configure the Apache web server.</p> <p>Enabling Mac and Linux clients to download LiveUpdate content using the Apache Web server as a reverse proxy</p> <p>See “Configuring a site to download content updates” on page 189.</p>
Group Update Provider to client computers (Windows only)	<p>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.</p> <p>Group Update Providers can distribute all types of LiveUpdate content except client software updates. Group Update Providers also cannot be used to update policies.</p>	<p>A Group Update Provider lets you reduce the load on the management server, and is easier to configure than an internal LiveUpdate server.</p> <p>Use a Group Update Provider for groups at remote locations with minimal bandwidth.</p> <p>See “Using Group Update Providers to distribute content to clients” on page 215.</p>

Table 8-2 Content distribution methods and when to use them (*continued*)

Method	Description	When to use it
<p>Internal LiveUpdate server to client computers (Windows, Mac, Linux)</p>	<p>Client computers can download updates directly from an internal LiveUpdate server that receives its updates from a Symantec LiveUpdate server.</p> <p>If necessary, you can set up several internal LiveUpdate servers and distribute the list to client computers.</p> <p>You change the schedule from LiveUpdate to the client in the LiveUpdate Settings policy.</p> <p>For more information about setting up an internal LiveUpdate server, see the <i>LiveUpdate Administrator User's Guide</i> at: Downloading LiveUpdate Administrator</p>	<p>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.</p> <p>Consider using an internal LiveUpdate server in the following situations:</p> <ul style="list-style-type: none"> ■ 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 <p>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.</p> <p>For more information see: LiveUpdate Administrator 2.x and Symantec Endpoint Protection Manager on the same computer</p> <p>See "Setting up an internal LiveUpdate server for Symantec Endpoint Protection clients" on page 211.</p>

Table 8-2 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.	<p>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.</p> <p>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.</p> <p>Note: Do not configure large numbers of managed, networked clients to pull updates from an external Symantec LiveUpdate server. This configuration consumes unnecessary bandwidth.</p> <p>See “Setting up an external LiveUpdate server for Symantec Endpoint Protection clients” on page 210.</p>
Third-party tool distribution (Windows only)	Third-party tools like Microsoft SMS let you distribute specific update files to clients.	<p>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.</p> <p>See “Distributing the content using third-party distribution tools” on page 231.</p>
Intelligent Updater (Windows only)	<p>Intelligent Updater files contain the virus and security risk content and intrusion prevention content that you can use to manually update clients.</p> <p>You can download the Intelligent Updater self-extracting files from the Symantec Web site.</p>	<p>You can use Intelligent Updater files if LiveUpdate is not available.</p> <p>See “Using Intelligent Updater files to update content on Windows computers” on page 227.</p> <p>To update other kinds of content, you must set up and configure a management server to download and to stage the update files.</p> <p>See “Using third-party distribution tools to update client computers” on page 228.</p>

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

Figure 8-1 Example distribution architecture for smaller networks

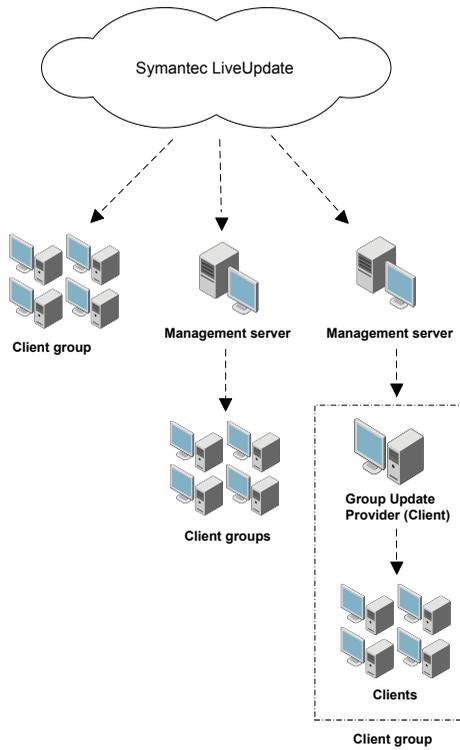
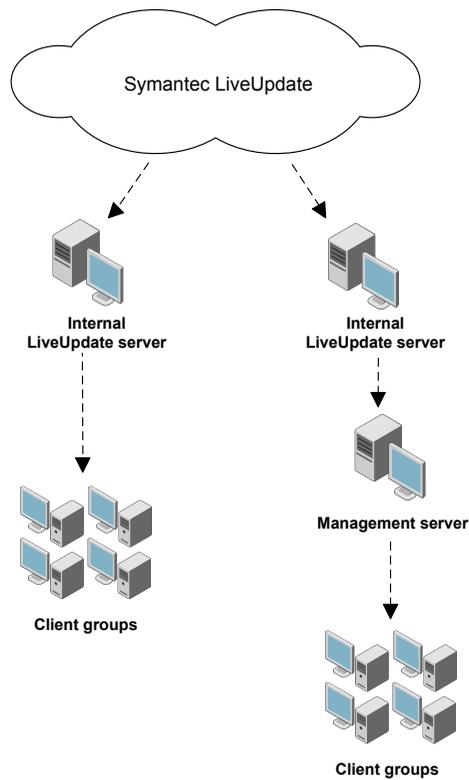


Figure 8-2 shows an example distribution architecture for larger networks.

Figure 8-2 Example distribution architecture for larger networks



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 8-3 Content distribution method based on Windows, Mac, and Linux clients

Platform	Method
Windows	<p>By default, the Windows client gets content from the management server.</p> <p>Windows clients can also get updates from the following sources:</p> <ul style="list-style-type: none"> ■ A LiveUpdate server (external or internal) See “Setting up an internal LiveUpdate server for Symantec Endpoint Protection clients” on page 211. See “Setting up an external LiveUpdate server for Symantec Endpoint Protection 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 231. ■ Intelligent Updater See “Using Intelligent Updater files to update content on Windows computers” on page 227. <p>See “Choose a distribution method to update content on clients” on page 182.</p>
Mac or Linux	<ul style="list-style-type: none"> ■ A LiveUpdate server (external or internal) ■ An Apache Web server that you configure as a reverse proxy See “Enabling Mac or Linux clients to download LiveUpdate content using the Apache Web server as a reverse proxy”

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 193.

See [“Configuring a site to download content updates”](#) on page 189.

See [“About the types of content that LiveUpdate can provide”](#) on page 197.

See [“Managing content updates”](#) on page 181.

Configuring a site to download content updates

When you configure a site to download LiveUpdate content, you have to make a number of decisions.

Table 8-4 Decisions about content downloads

Decision	Description
<p>What LiveUpdate server should serve the content to the site?</p>	<p>You can specify either an external Symantec LiveUpdate server (recommended), or one or more internal LiveUpdate servers that have previously been installed and configured.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>Downloading LiveUpdate Administrator</p> <p>See “Setting up an external LiveUpdate server for Symantec Endpoint Protection clients” on page 210.</p> <p>See “Setting up an internal LiveUpdate server for Symantec Endpoint Protection clients” on page 211.</p> <p>See “Choose a distribution method to update content on clients” on page 182.</p>

Table 8-4 Decisions about content downloads (*continued*)

Decision	Description
How many content revisions should the site store?	<p>In Symantec Endpoint Protection version 12.1.5 and later, LiveUpdate content revisions are stored differently on the management server than in previous versions. 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.</p> <p>The number of clients you select during the Symantec Endpoint Protection Manager installation defines the number of revisions the server stores.</p> <p>For each LiveUpdate content type, the default values are as follows:</p> <ul style="list-style-type: none"> ■ 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. <p>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.</p> <p>See “Configuring the content revisions that clients use” on page 205.</p>
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.
What content types should I download to the site?	<p>Make sure that the site downloads all content updates that are specified in your client LiveUpdate Content policies.</p> <p>See “About the types of content that LiveUpdate can provide” on page 197.</p> <p>See “Configuring the types of content used to update client computers” on page 196.</p>
What languages should be downloaded for product updates?	This setting applies to product updates only; the content updates are downloaded automatically for all languages.

Table 8-4 Decisions about content downloads (*continued*)

Decision	Description
What content size should be downloaded for definitions?	As of 12.1.6, you can download standard-size content or reduced-size content or both. If you select reduced content, any clients that require standard-size content cannot get updates from the management server. If you select standard content, any clients that require reduced-size content cannot get updates from the management server.

To configure a site to download updates

- 1 In the console, click **Admin**, and then click **Servers**.
- 2 Under **Servers**, right-click **Local Site**, and then click **Edit Site Properties**.
- 3 On the **LiveUpdate** tab, 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 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.symantecliveupdate.com** as the URL.

Note: If you use a UNC server, then LiveUpdate requires that you use the domain or workgroup as part of the user name.

If the computer is in a domain, use the format *domain_name\user_name*.

If the computer is in a workgroup, use the format *computer_name\user_name*.

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**.

Configuring the LiveUpdate download schedule for Symantec Endpoint Protection Manager

- 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 For 12.1.6, under **Content Size to Download**, decide whether to download and store standard-size definitions, reduced-size virus and spyware definitions, or both.

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 [“Managing content updates”](#) on page 181.

Configuring the LiveUpdate download schedule for Symantec Endpoint Protection Manager

You can adjust the schedule that Symantec Endpoint Protection Manager uses to download content updates from LiveUpdate to the management server. For example, you can change the default server schedule frequency from hourly to daily to save bandwidth.

To configure the schedule for LiveUpdate downloads to Symantec Endpoint Protection Manager

- 1 In the console, click **Admin > Servers**.
- 2 Click **Local Site (My Site)**.
- 3 Under **Tasks**, click **Edit Site Properties**.
- 4 In the **Server Properties** dialog box, on the **LiveUpdate** tab, click **Edit Schedule**.

5 Adjust the frequency and retry settings.

6 Click **OK**.

See [“Managing content updates”](#) on page 181.

Running LiveUpdate and downloading content to Symantec Endpoint Protection Manager immediately

You do not have to wait for your scheduled LiveUpdate downloads. You can manually download content updates to Symantec Endpoint Protection Manager. You can use either of the following procedures.

To run LiveUpdate and download content to Symantec Endpoint Protection Manager immediately

1 From the **Home Page**, select **Common Tasks** and then select **Run LiveUpdate**.

2 Click **Download**.

To manually download content updates to Symantec Endpoint Protection Manager

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

2 On the **Admin** page, click **Servers**, and then select the site.

3 Click **Download LiveUpdate content**.

4 In the **Download LiveUpdate Content** dialog box, review the properties, and then click **Download**.

If you need to change any of the properties, click **Cancel** and change the properties first.

See [“Configuring a site to download content updates”](#) on page 189.

See [“Managing content updates”](#) on page 181.

Mitigating network overloads for client update requests

Symantec Endpoint Protection Manager administrators must manage their networks for the critical but infrequent situation where too many clients simultaneously request full definition downloads from the management server or from a Group Update Provider. For example, if the management server encounters an error or runs out of disk space, the update 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 full package from the management server, or from the Group Update Provider.

To help prevent overloads on your network as a result of this situation, Symantec Endpoint Protection Manager now provides the following features:

- A notification when the server receives a specified number of requests for full definitions within a specified period of time.
You set the conditions for this notification to meet your network's needs. This notification lets you determine what constitutes an overload for your environment. You configure notifications at **Monitors > Notifications > Notification Conditions > Add/Edit**.
See "[Setting up administrator notifications](#)" on page 630.
- The ability to let clients get deltas for virus and spyware definitions from a LiveUpdate server if Symantec Endpoint Protection Manager can provide only full definitions. You configure this option at **Policies > LiveUpdate Server Settings > Advanced**.
To enable this option, you must also configure a LiveUpdate server in your LiveUpdate Settings policy. You configure this option at **Policies > LiveUpdate Server Settings > General**.
- The ability to block clients from downloading full definitions packages 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.
You configure this option at **Admin > Servers > server_name > Server Properties > Full Definitions Download**.

Checking LiveUpdate server activity

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

To check LiveUpdate server activity

- 1 In the console, click **Admin**.
- 2 On the **Admin** page, under **Tasks**, click **Servers** and select the site.
- 3 Click **Show the LiveUpdate Status**.
- 4 Click **Close**.

See "[Managing content updates](#)" on page 181.

Configuring Symantec Endpoint Protection Manager to connect to a proxy server to access the Internet and download content from Symantec LiveUpdate

If you want Symantec Endpoint Protection Manager to go through a proxy server to connect to the Internet, you must configure Symantec Endpoint Protection Manager to connect to the proxy server. A proxy server can add a layer of security because only the proxy server is connected directly to the Internet.

To configure Symantec Endpoint Protection Manager to connect to a proxy server to access the Internet and download content from Symantec LiveUpdate

- 1 In the console, click **Admin**, and then click **Servers**.
- 2 Under **Servers**, select the management server to which you want to connect a proxy server.
- 3 Under **Tasks**, click **Edit the server properties**.
- 4 On the **Proxy Server** tab, under either **HTTP Proxy Settings** or **FTP Proxy Settings**, for **Proxy usage**, select **Use custom proxy settings**.
- 5 Type in the proxy settings.
For more information on these settings, click **Help**.
- 6 Click **OK**.

See [“Managing content updates”](#) on page 181.

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 [“Managing content updates”](#) on page 181.

Configuring the types of content used to update client computers

The LiveUpdate Content policy specifies the content types that clients are permitted to check for and install. Rolling back content to an old revision can be useful in troubleshooting situations

Note: Use this feature very carefully. Unchecking a content type means that the feature is not kept up-to-date on the client. This can potentially put your clients at greater risk.

To configure the update content for client computers

- 1 In the console, click **Policies**.
- 2 Under **Policies**, click **LiveUpdate**, and then click the **LiveUpdate Content** tab.
- 3 Right-click the content policy that you want, and then click **Edit**.
- 4 Under **Windows Settings**, click **Security Definitions**.
- 5 Check the types of content updates that you want clients to download and install, and uncheck the types that you don't want.

Note: If you have Mac clients, they can install only updates to virus and spyware definitions and intrusion prevention signatures. These options, under **Mac Settings, Security Definitions**, are enabled by default.

- 6 Optionally, for each update, you can use the latest available content, or select a specific revision from a list of available versions.
- 7 Click **OK**.

If you have not already assigned this policy to groups and locations, then you must assign the policy to have it take effect.

See [“Configuring a site to download content updates”](#) on page 189.

See [“Managing content updates”](#) on page 181.

See [“Configuring the content revisions that clients use”](#) on page 205.

About the types of content that LiveUpdate can provide

The types of content that LiveUpdate can provide include virus and spyware definitions, Intrusion Prevention System signatures, and product updates. To control the content types that your client computers download, you use a LiveUpdate Content policy. To control the content types that the default management server downloads to distribute to clients, you configure the properties settings for the site. If content is selected in a LiveUpdate policy but is not selected in the site properties, that content is not delivered to the clients.

Configuring the types of content used to update client computers

Note: Typically, you should not need to restrict the content that Symantec Endpoint Protection Manager downloads. Be careful to only turn off a type of content if you are certain that you do not need it.

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

[Table 8-5](#) lists the types of content that you can configure in Symantec Endpoint Protection Manager to download to clients.

Table 8-5 The content types that you can configure for download to the clients

Content type	Description
Product updates	<p>Product updates are improvements to the installed client software. These updates are usually created to extend the operating system or hardware compatibility, adjust performance issues, or fix product errors. Product updates are released on an as-needed basis. Clients can receive product updates directly from a LiveUpdate server. Managed clients can also receive product updates from Symantec Endpoint Protection Manager.</p> <ul style="list-style-type: none"> ■ The Product Update Settings parameter in the Advanced Settings of a LiveUpdate Settings policy lets you control your client software versions. This choice is not configured in a LiveUpdate Content policy. When this setting is enabled, client software can be updated through LiveUpdate. ■ The Symantec Endpoint Protection Manager downloads client updates by default through LiveUpdate. This setting can be disabled in the site properties for Symantec Endpoint Protection Manager. When an update is downloaded, it appears in the Client Install Packages pane. You can then select the package, and use the Upgrade Clients with Package feature for your Windows clients. <p>You can use the Client Deployment Wizard to update your Mac and Linux clients. Web link and email creates a package and sends the download URL to the intended email recipients. Save package builds and exports an installation package. This package can then be deployed with a third-party tool, or placed in a network location for download and manual installation.</p>
Virus and Spyware definitions	<p>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.</p>
SONAR heuristic signatures	<p>Protects against zero-day attack threats.</p>
TruScan proactive threat scan commercial application list	<p>Includes the legitimate commercial applications that have generated false positives in the past. These are used for backward compatibility when you manage 11.0 clients.</p>

Table 8-5 The content types that you can configure for download to the clients
(continued)

Content type	Description
Intrusion Prevention signatures	Protects against network threats and supports the intrusion prevention and detection engines.
Submission Control signatures	Controls the flow of submissions to Symantec Security Response.
Reputation Settings	Includes the updates to the reputation data that is used in protection.
Host Integrity content	Includes the templates of predefined requirements that enforce updated patches and security measures on the client computer. LiveUpdate downloads templates for the computers that run Windows operating systems and Mac operating systems. See “Adding a custom requirement from a template” on page 583.

Note: You cannot exclude all types of content. For example, the **Extended File Attributes and Signatures** that are used to control root certificate and signer information are always downloaded.

See [“Managing content updates”](#) on page 181.

See [“Choose a distribution method to update content on clients”](#) on page 182.

See [“Configuring the types of content used to update client computers”](#) on page 196.

[Table 8-6](#) lists the features that need regular updates and the types of content that each feature needs.

Table 8-6 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	<ul style="list-style-type: none"> ■ Virus and Spyware Definitions ■ SONAR Definitions When you configure content types for download in Site Properties, these are called SONAR heuristic signatures. ■ Symantec Whitelist When you configure a site to download content, this content type is called TruScan proactive threat scan commercial application list. ■ Revocation Data (downloaded by default, not configurable from Symantec Endpoint Protection Manager) ■ Centralized Reputation Settings When you configure content types for download in Site Properties, this content type is called Reputation Settings. ■ Submission Control signatures ■ Auto-Protect portal list ■ Power Eraser definitions
Virus and Spyware Protection > Download Protection	<ul style="list-style-type: none"> ■ Virus and Spyware Definitions ■ SONAR Definitions When you configure content types for download in Site Properties, these are called SONAR heuristic signatures. ■ Symantec Whitelist When you configure a site to download content, this content type is called TruScan proactive threat scan commercial application list. ■ Revocation Data (downloaded by default, not configurable from Symantec Endpoint Protection Manager) ■ Centralized Reputation Settings When you configure content types for download in Site Properties, this content type is called Reputation Settings. ■ Intrusion Prevention signatures When you select this option to download, it includes updates to both the Intrusion Prevention signatures and the Intrusion Prevention engines. ■ Submission Control signatures ■ Auto-Protect portal list ■ Power Eraser definitions

Table 8-6 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	<ul style="list-style-type: none"> ■ Virus and Spyware Definitions ■ SONAR Definitions When you configure content types for download in Site Properties, these are called SONAR heuristic signatures. ■ Symantec Whitelist When you configure a site to download content, this content type is called TruScan proactive threat scan commercial application list. ■ Revocation Data (downloaded by default, not configurable from Symantec Endpoint Protection Manager) ■ Centralized Reputation Settings When you configure content types for download in Site Properties, this content type is called Reputation Settings. ■ Submission Control signatures ■ Auto-Protect Portal List ■ Power Eraser Definitions
Virus and Spyware Protection > Notes Scanner	<ul style="list-style-type: none"> ■ Virus and Spyware Definitions ■ SONAR Definitions When you configure content types for download in Site Properties, these are called SONAR heuristic signatures. ■ Symantec Whitelist When you configure a site to download content, this content type is called TruScan proactive threat scan commercial application list. ■ Revocation Data (downloaded by default, not configurable from Symantec Endpoint Protection Manager) ■ Centralized Reputation Settings When you configure content types for download in Site Properties, this content type is called Reputation Settings. ■ Submission Control signatures ■ Auto-Protect Portal List ■ Power Eraser Definitions
Proactive Threat Protection > SONAR	SONAR Definitions Submission Control signatures When you configure content types for download in Symantec Endpoint Protection Manager, these are called SONAR heuristic signatures.
Proactive Threat Protection > Application and Device Control	Submission Control signatures

Table 8-6 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
Network Threat Protection > Intrusion Prevention	Intrusion Prevention signatures Submission Control signatures Note: When you select this option to download, it includes updates to both the intrusion prevention signatures and the Intrusion Prevention engines.
Network Threat Protection > Firewall	Submission Control signatures
Network Access Control	Host Integrity content Submission Control signatures

Note: You cannot configure **Extended File Attributes and Signatures** and **Submission control signatures**. They are always installed.

Configuring the LiveUpdate download schedule for 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 [“Setting up an external LiveUpdate server for Symantec Endpoint Protection clients”](#) on page 210.

See [“Setting up an internal LiveUpdate server for Symantec Endpoint Protection clients”](#) on page 211.

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 208.

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 [“Managing content updates”](#) on page 181.

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 [“Configuring the content revisions that clients use”](#) on page 205.

See [“Configuring the LiveUpdate download schedule for client computers”](#) on page 202.

Configuring the content revisions that clients use

You might want to specify a particular content revision in your LiveUpdate Content policy. For example, you can test the latest revision before you roll it out to clients.

Note: If you want to keep strict control of the client software revisions that your clients use, do not enable them to download product updates.

See [“Configuring the amount of control that users have over LiveUpdate”](#) on page 204.

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

To configure clients to use a specific content version

- 1 In the console, click **Policies**.
- 2 Under **Policies**, click **LiveUpdate**.
- 3 Click the **LiveUpdate Content** tab.
- 4 Right-click the LiveUpdate Content policy that you want and then click **Edit**.

- 5 Under **Windows Settings**, click **Security Definitions**.
- 6 Under the type of content that you want to roll back, click **Select a revision**.
- 7 Click **Edit** and select the revision that you want to roll back to from the **Revision** drop-down list.
- 8 Click **OK**.

See [“Managing content updates”](#) on page 181.

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 207.

See [“Randomizing content downloads from a LiveUpdate server”](#) on page 208.

See [“Setting up an internal LiveUpdate server for Symantec Endpoint Protection clients”](#) on page 211.

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 208.

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 206.

See [“Setting up an internal LiveUpdate server for Symantec Endpoint Protection clients”](#) on page 211.

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 207.

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 206.

See [“Setting up an internal LiveUpdate server for Symantec Endpoint Protection clients”](#) on page 211.

Configuring 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 client updates to run when client computers are idle

- 1 Click **Policies**.
- 2 Under **Policies**, click **LiveUpdate**.
- 3 On the **LiveUpdate Settings** tab, right-click the policy that you want to edit, and then click **Edit**.
- 4 Under **Windows Settings**, click **Schedule**.
- 5 Check **Delay scheduled LiveUpdate until the computer is idle. Overdue sessions will run unconditionally**.
- 6 Click **OK**.

See [“Configuring the LiveUpdate download schedule for client computers”](#) on page 202.

See [“Configuring client updates to run when definitions are old or the computer has been disconnected”](#) on page 210.

Configuring 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 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 for client computers”](#) on page 202.

See [“Configuring client updates to run when client computers are idle”](#) on page 209.

Setting up an external LiveUpdate server for Symantec Endpoint Protection clients

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 182.

[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 195.

To set up an external LiveUpdate server for Windows, Mac, or Linux clients

- 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 [“Managing content updates”](#) on page 181.

Setting up an internal LiveUpdate server for Symantec Endpoint Protection clients

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:

Setting up an internal LiveUpdate server for Symantec Endpoint Protection clients

- 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 195.

To configure Windows clients to use an internal LiveUpdate server

- 1 Under **Policies**, click **LiveUpdate**.
- 2 On the **LiveUpdate Settings** tab, right-click the policy that you want and then click **Edit**.
- 3 Under **Windows Settings**, click **Server Settings**.
- 4 In the **Server Settings** pane, check **Use a LiveUpdate server**.
- 5 Click **Use a specified internal LiveUpdate server**, and then click **Add**.
- 6 In the **Add LiveUpdate Server** dialog box, type the information that you need to identify and communicate with the server that you want to use.

For example, for the URL:

- If you use the FTP method (recommended), type the FTP address for the server. For example: ftp://myliveupdateserver.com
- If you use the HTTP method, type the URL for the server. For example: http://myliveupdateserver.com or http://2.168.133.11/Export/Home/LUDepot
- If you use the LAN method, type the server UNC path name. For example, \\Myserver\LUDepot

- 7 If required, type in a user name and password for the server.

Note: If you use a UNC server, then LiveUpdate requires that you use the domain or workgroup in addition to the user name. If the computer is part of a domain, use the format *domain_name\user_name*

If the computer is part of a workgroup, use the format *computer_name\user_name*.

- 8 Under **LiveUpdate Policy**, click **Schedule** to set up a schedule for updates through LiveUpdate.

See [“Configuring the LiveUpdate download schedule for client computers”](#) on page 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: http://myliveupdateserver.com or http://2.168.133.11/Export/Home/LUDepot

Setting up an internal LiveUpdate server for Symantec Endpoint Protection clients

- 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: http://myliveupdateserver.com or http://2.168.133.11:7070/export/home.
- 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 208.

See [“Configuring client updates to run when client computers are idle”](#) on page 209.

See [“Choose a distribution method to update content on clients”](#) on page 182.

Using Group Update Providers to distribute content to clients

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

One advantage of Group Update Provider use is that it helps you to conserve bandwidth by offloading processing power from the server to the Group Update Provider. Group Update Providers are ideal for delivering content updates to clients that have limited network access to the server. You can use a Group Update Provider to conserve bandwidth to clients in a remote location over a slow link. Setting up a Group Update Provider is easier than setting up an internal LiveUpdate server. Group Update Providers are less resource-intensive and so reduce the load on the management servers.

You use a LiveUpdate Settings policy to configure Group Update Providers.

Table 8-7 Tasks to configure and use Group Update Providers

Step	Action	Description
Step 1	Understand the differences between the types of Group Update Providers that you can configure	<p>A single Group Update Provider is a dedicated client computer that provides content for one or more groups of clients. Multiple Group Update Providers use a set of rules, or criteria, to elect themselves to serve groups of clients in their subnet. An explicit list of Group Update Providers lets clients connect to Group Update Providers that are on subnets other than the client's own subnet. You use the explicit list to map the single Group Update Providers and multiple Group Update Providers to the client subnets.</p> <p>The types of Group Update Provider that you choose to configure depends on your network and the clients on that network.</p> <p>See "About the types of Group Update Providers" on page 216.</p> <p>See "About the effects of configuring more than one type of Group Update Provider in your network" on page 220.</p> <p>See "About configuring rules for multiple Group Update Providers" on page 222.</p>
Step 2	Verify client communication	<p>Before you configure Group Update Providers, verify that the clients can receive content updates from the server. Resolve any client-server communication problems.</p> <p>You can view client-server activity in the System logs on the Logs tab of the Monitors page.</p> <p>See "Troubleshooting communication problems between the management server and the client" on page 745.</p>

Table 8-7 Tasks to configure and use Group Update Providers (*continued*)

Step	Action	Description
Step 3	Configure Group Update Providers in one or more LiveUpdate Settings policies	<p>You configure Group Update Providers by specifying Server Settings in the LiveUpdate Settings policy. You can configure a single Group Update Provider, an explicit list of Group Update Providers, or multiple Group Update Providers.</p> <p>See “Configuring Group Update Providers” on page 223.</p>
Step 4	Assign the LiveUpdate Settings policy to groups	<p>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.</p> <p>For a single Group Update Provider, you assign one LiveUpdate Settings policy per group per site.</p> <p>For multiple Group Update Providers and explicit lists of Group Update Providers, you assign one LiveUpdate Settings policy to multiple groups across subnets.</p> <p>See “Assigning a policy to a group” on page 323.</p>
Step 5	Verify that clients are designated as Group Update Providers	<p>You can view the client computers that are designated as Group Update Providers. You can search client computers to view a list of Group Update Providers. You can also click a client computer on the Clients page and view its properties to see whether or not it is a Group Update Provider.</p> <p>See “Searching for the clients that act as Group Update Providers” on page 226.</p>

About the types of Group Update Providers

You can configure several different types of Group Update Providers in the LiveUpdate Settings policy: a single Group Update Provider, an explicit list of Group Update Providers, and multiple Group Update Providers. The types of Group Update Provider are not mutually exclusive. You can configure one or more types of Group Update Provider per policy.

- **Single Group Update Provider**
 A single Group Update Provider is a dedicated client computer that provides content for one or more groups of clients. A single Group Update Provider can be a client computer in any group. To configure a single Group Update Provider, you specify the IP address or host name of the client computer that you want to designate as the Group Update Provider. A single Group Update Provider is a static Group Update Provider.
 Configuring a single Group Update Provider turns a single client into a Group Update Provider.

- Explicit Group Update Providers list

You can configure an explicit list of Group Update Providers for clients to connect to Group Update Providers that are on other subnets. Clients that change location frequently can then roam to the closest Group Update Provider on the list.

An explicit Group Update Providers list does not turn clients into Group Update Providers. You use an explicit Group Update Provider list to map the client subnet network addresses to the Group Update Providers. You identify the Group Update Providers by any of following means:

- IP address
- Host name
- Subnet

Explicit Group Update Providers can be static or dynamic, depending on how you configure them. If you use an IP address or a host name to configure an explicit Group Update Provider, then it is a static Group Update Provider. This difference affects how Group Update Providers act in those networks that mix clients and managers from the current release and a legacy release.

Note: A legacy release is any release earlier than the most current.

If you use a subnet to designate a Group Update Provider, it is dynamic, as clients search for a Group Update Provider on that subnet.

Note: This subnet is the Group Update Provider subnet network address, which is sometimes also referred to as the network prefix or network ID.

- Multiple Group Update Providers list

Multiple Group Update Providers use a set of rules, or criteria, to elect themselves to serve groups of clients in their own subnets. To configure multiple Group Update Providers, you specify the criteria that client computers must meet to qualify as a Group Update Provider. You can use a host name or IP address, registry keys, or operating system as criteria. If a client computer meets the criteria, the Symantec Endpoint Protection Manager adds the client to a global list of Group Update Providers. Symantec Endpoint Protection Manager then makes the global list available to all the clients in the network. Clients check the list and choose the Group Update Providers that are located in their own subnet. Multiple Group Update Providers are dynamic Group Update Providers.

Configuring multiple Group Update Providers turns multiple clients into Group Update Providers.

Configuring single or multiple Group Update Providers in a LiveUpdate Settings policy performs the following functions:

- It specifies which clients with this policy are to act as Group Update Providers.
- It specifies which Group Update Provider or Providers the clients with this policy should use for content updates.

Configuring an Explicit Group Update Provider list performs only one function:

- It specifies which Providers the clients with this policy should use for content updates. It maps Group Update Providers on subnets for use by clients on different subnets.
- It does not specify any clients as Group Update Providers.

Although it does not turn clients into Group Update Providers, you can still configure and apply a policy that contains only an explicit provider list. However, you must then have a single Group Update Provider or multiple Group Update Providers configured in another policy in the Symantec Endpoint Protection Manager. Or, you can have both types configured in other policies.

Note: 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. This action occurs because Symantec Endpoint Protection Manager constructs a global list. For Example, clients on a different subnet can end up using a Group Update Provider that you configured as a single static provider. This usage occurs if the configured subnet mapping in an explicit list in another policy matches it.

See [“About the effects of configuring more than one type of Group Update Provider in your network”](#) on page 220.

If a client cannot obtain its update through any of the Group Update Providers, it can then optionally try to update from the Symantec Endpoint Protection Manager.

Table 8-8 How the explicit type of Group Update Provider can be used based on the software versions in the network

Symantec Endpoint Protection Manager Version	Client Versions	Group Update Provider Client Version	Types of Group Update Provider that you can use
12.1.2 and later	12.1.1 and earlier	Any	You can configure single or multiple Group Update Providers, but not explicit Group Update Providers because the clients do not support them.

Table 8-8 How the explicit type of Group Update Provider can be used based on the software versions in the network (*continued*)

Symantec Endpoint Protection Manager Version	Client Versions	Group Update Provider Client Version	Types of Group Update Provider that you can use
12.1.1 and earlier	Any	Any	You can configure single or multiple Group Update Providers, but not any type of explicit Group Update Provider because they are not available in the Symantec Endpoint Protection Manager.

The types of Group Update Providers that you configure depend on how your network is set up and whether your network includes legacy clients.

Table 8-9 When to use particular types of Group Update Provider

Group Update Provider Type	When to use
Single	<p>Use a single Group Update Provider when you want to use the same Group Update Provider for all your client computers. All client computers are on the same subnet.</p> <p>You can use a single LiveUpdate Settings policy to specify a static IP address or host name for a single Group Update Provider. However, you must change the IP address in the policy if the clients that serve as single Group Update Providers change locations.</p> <p>If you want to use different single Group Update Providers in different groups, you must create a separate LiveUpdate Settings policy for each group.</p>
Explicit list	<p>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.</p> <p>Note: Clients from releases earlier than 12.1.2 do not support the use of explicit Group Update Provider lists. Clients that communicate with Symantec Endpoint Protection Manager versions 12.1 and earlier do not receive any information about explicit Group Update Provider lists.</p>

Table 8-9 When to use particular types of Group Update Provider (*continued*)

Group Update Provider Type	When to use
Multiple	<p>Use multiple Group Update Providers when your network includes any of the following scenarios:</p> <ul style="list-style-type: none"> ■ 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. <p>Multiple Group Update Providers are supported on all versions of Symantec Endpoint Protection 12.1.</p>

See [“Using Group Update Providers to distribute content to clients”](#) on page 215.
 See [“About configuring rules for multiple Group Update Providers”](#) on page 222.
 See [“Configuring Group Update Providers”](#) on page 223.

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 `C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\data\outbox\agent\gup\globallist.xml` on 64-bit operating systems, or `C:\Program Files\Symantec\Symantec Endpoint Protection Manager\data\outbox\agent\gup\globallist.xml` on 32-bit operating systems. Symantec Endpoint Protection Manager provides this global list to any client that asks for it so that the client can determine which Group Update Provider it should use. Because of this process, clients that have policies with only multiple or explicit Group Update Providers configured can also use single Group Update Providers, if the single provider meets the explicit mapping criterion. This phenomenon can occur because single providers are a part of the global list of providers that the clients get from their Symantec Endpoint Protection Manager.

So, all of the Group Update Providers that are configured in any of the policies on a Symantec Endpoint Protection Manager are potentially available for clients' use. If you apply a policy that contains only an explicit Group Update Provider list to the clients in a group, all of the clients in the group attempt to use the Group Update Providers that are in the Symantec Endpoint Protection Manager global Group Update Provider list that meet the explicit mapping criteria.

Note: A Symantec Endpoint Protection client may have multiple IP addresses. Symantec Endpoint Protection considers all IP addresses when it matches to a Group Update Provider. So, the IP address that the policy matches is not always bound to the interface that the client uses to communicate with the Symantec Endpoint Protection Manager and the Group Update Provider.

If all types of Group Update Providers are configured in the policies on a Symantec Endpoint Protection Manager, then clients try to connect to Group Update Providers in the global list in the following order:

- Providers on the **Multiple Group Update Providers** list, in order
- Providers on the **Explicit Group Update Providers** list, in order
- The Provider that is configured as a **Single Group Update Provider**

You can configure the following types of explicit mapping criteria:

- IP address: Clients in subnet A should use the Group Update Provider that has the IP address **x.x.x.x**.
- Host name: Clients in subnet A should use the Group Update Provider that has the host name **xxxx**.
- Subnet network address: Clients in subnet A should use any Group Update Provider that resides on **subnet B**.

Multiple mapping criteria can be used in an explicit Group Update Provider list in a single policy. Symantec recommends that you be very careful how you configure multiple mapping criteria to avoid unintended consequences. For example, you can strand your clients without a means of obtaining updates if you misconfigure an explicit mapping.

Consider a scenario with the following multiple explicit mapping criteria configured in a single policy:

- If a client is in subnet 10.1.2.0, use the Group Update Provider that has IP address 10.2.2.24
- If a client is in subnet 10.1.2.0, use the Group Update Provider that has IP address 10.2.2.25

- If a client is in subnet 10.1.2.0, use the Group Update Provider that has host name **SomeMachine**
- If a client is in subnet 10.1.2.0, use any Group Update Provider on subnet 10.5.12.0
- If a client is in subnet 10.6.1.0, use any Group Update Provider on subnet 10.10.10.0

With this explicit Group Update Provider policy, if a client is in subnet 10.1.2.0, the first four rules apply; the fifth rule does not. If the client is in a subnet for which no mapping is specified, such as 10.15.1.0, then none of the rules apply to that client. That client's policy says to use an explicit Group Update Provider list, but there is no mapping that the client can use based on these rules. If you also disabled that client's ability to download updates from Symantec Endpoint Protection Manager and the Symantec LiveUpdate server, then that client has no usable update method.

About configuring rules for multiple Group Update Providers

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

Rules are structured as follows:

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

Table 8-10 Rule types

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

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

- Multiple rule sets are OR'ed.
A client must match at least one rule set to act as a Group Update Provider.
- Multiple rules are AND'ed.
A client must match every rule that is specified in a rule set to act as a Group Update Provider.
- Multiple values for a rule condition are OR'ed.
A client must match one of the values in a rule condition to act as a Group Update Provider.

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

See [“Using Group Update Providers to distribute content to clients”](#) on page 215.

See [“About the types of Group Update Providers”](#) on page 216.

See [“Configuring Group Update Providers”](#) on page 223.

Configuring Group Update Providers

You configure Group Update Providers in the LiveUpdate Settings policy.

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

You can configure the maximum amount of time that clients try to download updates from a Group Update Provider before they try to get updates from their default management server. If you set this time to 15 minutes, this means that the client computer must try to download continuously for 15 minutes with no success.

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

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

You can configure multiple Group Update Providers by specifying the criteria that clients use to determine if they qualify to act as a Group Update Provider.

You can configure an explicit list of Group Update Providers for roaming clients to use.

See [“Using Group Update Providers to distribute content to clients”](#) on page 215.

See [“About the types of Group Update Providers”](#) on page 216.

To configure a Group Update Provider

- 1 In the console, click **Policies**.
- 2 Under **Policies**, click **LiveUpdate**.
- 3 On the **LiveUpdate Settings** tab, right-click the policy that you want and then click **Edit**.
- 4 In the **LiveUpdate Settings Policy** window, click **Server Settings**.
- 5 Under **Internal or External LiveUpdate Server**, check **Use the default management server**.
- 6 Under **Group Update Provider**, check **Use a Group Update Provider**.
- 7 Click **Group Update Provider**.
- 8 Do one of the following tasks:
 - Follow the steps in [To configure a single Group Update Provider](#).
 - Follow the steps in [To configure multiple Group Update Providers](#).
- 9 In the **Group Update Provider** dialog box, configure the options to control how content is downloaded and stored on the Group Update Provider computer.
Click **Help** for information about content downloads.
- 10 Click **OK**.

To configure a single Group Update Provider

- 1 In the **Group Update Provider** dialog box, under **Group Update Provider Selection for Client**, click **Single Group Update Provider IP address or host name**.
- 2 In the **Single Group Update Provider IP address or host name** box, type the IP address or host name of the client computer that acts as the single Group Update Provider.
Click **Help** for information about the IP address or host name.
- 3 Return to the procedure to configure a Group Update Provider.

To configure multiple Group Update Providers

- 1 In the **Group Update Provider** dialog box, under **Group Update Provider Selection for Client**, click **Multiple Group Update Providers**.
- 2 Click **Configure Group Update Provider List**.
- 3 In the **Group Update Provider List** dialog box, select the tree node **Group Update Provider**.
- 4 Click **Add** to add a rule set.
- 5 In the **Specify Group Update Provider Rule Criteria** dialog box, in the **Check** drop-down list, select one of the following options:
 - **Computer IP Address or Host Name**
 - **Registry Keys**
 - **Operating System**
- 6 If you selected **Computer IP Address or Host Name** or **Registry Keys**, click **Add**.
- 7 Type or select the IP address or host name, Windows registry key, or operating system information.

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

See [“About configuring rules for multiple Group Update Providers”](#) on page 222.
- 8 Click **OK** until you return to the **Group Update Provider List** dialog box, where you can optionally add more rule sets.
- 9 Click **OK**.
- 10 Return to the procedure to configure a Group Update Provider.

When you configure an explicit list of Group Update Providers, you can specify that Symantec Endpoint Protection clients with IP addresses that fall on a particular subnet should use a particular Group Update Provider. Note that a client may have multiple IP addresses and that Symantec Endpoint Protection considers all of its IP addresses when it matches the Group Update Provider to use. So, the IP address that the policy matches to is not necessarily bound to the interface that the client uses to communicate with the Group Update Provider.

For example, suppose that a client has IP address A, which it uses to communicate with the Symantec Endpoint Protection Manager and with the Group Update Provider. This same client also has IP address B, which is the one that matches the Explicit Group Update Provider that you have configured in the LiveUpdate Settings policy for this client. The client can choose to use a Group Update Provider based on the address B, even though that is not the address that it uses to communicate with the Group Update Provider.

To configure an explicit list of Group Update Providers

- 1 In the console, click **Policies**.
- 2 Under **Policies**, click **LiveUpdate**.
- 3 On the **LiveUpdate Settings** tab, click **Add a LiveUpdate Settings policy**, or right-click the policy that you want and then click **Edit**.
- 4 In the **LiveUpdate Settings Policy** window, click **Server Settings**.
- 5 Under **Internal or External LiveUpdate Server**, check **Use the default management server**.
- 6 Under **Group Update Provider**, check **Use a Group Update Provider**.
- 7 Click **Group Update Provider**.
- 8 In the **Group Update Provider** dialog box, under **Group Update Provider Selection for Client**, click **Explicit Group Update Providers for roaming clients**, and then click **Configure Explicit Group Update Provider List**.
- 9 Click **Add**.
- 10 In the **Add Explicit Group Update Provider** dialog box, type in the client subnet that you want to map these Group Update Providers to.
- 11 Under **Explicit Group Provider Settings**, select the **Type** of mapping you want to set up: based on the IP address, the host name, or the Group Update Provider's network address.
- 12 Type in the necessary settings for the type of mapping you selected, and then click **OK**.

Searching for the clients that act as Group Update Providers

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

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

To search for the clients that act as Group Update Providers

- 1 In the console, click **Clients**.
- 2 On the **Clients** tab, in the **View** box, select **Client status**.
- 3 In the **Tasks** pane, click **Search clients**.
- 4 In the **Find** drop-down list, select **Computers**.

- 5 In the **In Group** box, specify the group name.
 - 6 Under **Search Criteria**, click in the **Search Field** column and select **Group Update Provider**.
 - 7 Under **Search Criteria**, click in the **Comparison Operator** column and select **=**.
 - 8 Under **Search Criteria**, click in the **Value** column and select **True**.
Click **Help** for information on the search criteria.
 - 9 Click **Search**.
- See [“Using Group Update Providers to distribute content to clients”](#) on page 215.

Using Intelligent Updater files to update content on Windows computers

Symantec recommends that client computers use LiveUpdate to update content on 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 Windows clients with some types of content. The Intelligent Updater .exe files are designed to update clients only. Intelligent Updater files do not contain the information that a Symantec Endpoint Protection Manager needs to update its managed clients.

An Intelligent Updater file is a self-executing file that contains virus and spyware definitions, SONAR definitions, and intrusion prevention signatures.

An Intelligent Updater file does not provide updates for any other type of content. After you download the file, you can use your preferred distribution method to distribute the updates to your clients.

Note: Intelligent Updater does not support the Extended file attributes and signatures, 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 site:
ftp://ftp.symantec.com/AVDEFS/symantec_antivirus_corp/
- 2 On the FTP site, click the appropriate product file with the .exe extension.
- 3 When you are prompted for a location in which to save the file, select a folder on your hard drive.
- 4 Distribute the file to the client computers using your preferred distribution method.

To install the virus and security risk definitions files on a client computer

- 1 On the client computer, locate the Intelligent Updater file that was distributed to the client.
- 2 Double-click the .exe file and follow the on-screen instructions.

See [“Choose a distribution method to update content on clients”](#) on page 182.

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.

[Table 8-11](#) outlines the tasks that you need to perform to use a third-party distribution tool.

Note: Before you set up the use of third-party distribution tools, you must have already installed Symantec Endpoint Protection Manager and the client computers that you want to update.

Table 8-11 Tasks to set up the use of third-party distribution tools for updates

Task	Description
Configure Symantec Endpoint Protection Manager to receive content updates.	<p>You can configure the management server either to receive content updates automatically or manually.</p> <p>See “Configuring a site to download content updates” on page 189.</p> <p>See “Managing content updates” on page 181.</p>
Configure the group's LiveUpdate Settings policy to allow third-party content update distribution.	<p>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.</p> <p>See “Configuring a LiveUpdate Settings policy to allow third-party content distribution to managed clients” on page 229.</p>

Table 8-11 Tasks to set up the use of third-party distribution tools for updates
(continued)

Task	Description
Prepare unmanaged clients to receive updates from third-party distribution tools.	<p>If you want to use third-party distribution tools to update unmanaged clients, you must first create a registry key on each unmanaged client.</p> <p>See “Preparing unmanaged clients to receive updates from third-party distribution tools” on page 230.</p>
Locate, copy, and distribute the content.	<p>Each Symantec Endpoint Protection Manager client group has an index2.dax file that is located on the computer that runs Symantec Endpoint Protection Manager. These files are located in subfolders under the <i>Symantec Endpoint Protection Manager installation\data\outbox\agent</i> folder. To update clients, you need to use the index2.dax files.</p> <p>See “Configuring a site to download content updates” on page 189.</p> <p>See “Distributing the content using third-party distribution tools” on page 231.</p>

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
`drive:\ProgramData\Symantec\Symantec Endpoint Protection\CurrentVersion\inbox`
- Pre-Vista operating systems
`drive:\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 [“Setting up an internal LiveUpdate server for Symantec Endpoint Protection clients”](#) on page 211.

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
`drive:\ProgramData\Symantec\Symantec Endpoint Protection\
CurrentVersion\inbox`
- Pre-Vista operating systems
`drive:\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 228.

See [“Distributing the content using third-party distribution tools”](#) on page 231.

Distributing the content using third-party distribution tools

To use third-party distribution tools to distribute content to client computers, you need to use the index2.dax file. The LiveUpdate-related content in the index2 file includes a set of GUIDs called content monikers and their associated sequence numbers. Each content moniker corresponds to a particular content type. Each sequence number in the index2 file corresponds to a revision of a particular content type. Depending on the protection features that you have installed, you need to determine which of the content types you need.

See [“About the types of content that LiveUpdate can provide”](#) on page 197.

Note: Content monikers typically change with each major release. At times, they may also change for a minor release. Symantec does not typically change the monikers for Release Updates or Maintenance Patches.

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

For example, you might see the following entry:

```
{535CB6A4-441F-4e8a-A897-804CD859100E}: SEPC Virus Definitions Win32 12.1 RU6
```

Each Symantec Endpoint Protection Manager client group has its own index2 file. The index2 file for each client group is found in a folder for that group. The folders for client groups can be found in the Symantec Endpoint Protection Manager installation folder, in \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.

Note: January 5, 2015 was the End of Support Life for Symantec Endpoint Protection 11.0. Content updates for Symantec Endpoint Protection 11.0 ceased on this date. You should upgrade any remaining Symantec Endpoint Protection 11.0 clients to the latest version of Symantec Endpoint Protection.

[Symantec Endpoint Protection 11.0.x End of Support Life](#)

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 one of the following folders:
 - `C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\data\outbox\agent (64-bit operating systems)`
 - `C:\Program Files\Symantec\Symantec Endpoint Protection Manager\data\outbox\agent (32-bit operating systems)`
- 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 one of the following folders:
 - `C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\inetpub\content (64-bit operating systems)`
 - `C:\Program Files\Symantec\Symantec Endpoint Protection Manager\inetpub\content (32-bit operating systems)`
- 8 Open and read `ContentInfo.txt` to discover the content that each *target moniker* folder contains.

The contents of each directory is `target moniker\sequence number\full.zip|full`.
- 9 Copy the contents of each `\target moniker` folder to your working folder such as `\Work_Dir`.

- 10 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 228.

See [“Preparing unmanaged clients to receive updates from third-party distribution tools”](#) on page 230.

Managing groups, clients, and administrators

- [Chapter 9. Managing groups of client computers](#)
- [Chapter 10. Managing clients](#)
- [Chapter 11. Managing remote clients](#)
- [Chapter 12. Managing administrator accounts and passwords](#)
- [Chapter 13. Managing domains](#)

Managing groups of client computers

This chapter includes the following topics:

- [Managing groups of clients](#)
- [How you can structure groups](#)
- [Adding a group](#)
- [Importing existing groups and computers from an Active Directory or an LDAP server](#)
- [Assigning clients to groups before you install the client software](#)
- [Disabling and enabling a group's inheritance](#)
- [Blocking client computers from being added to groups](#)
- [Moving a client computer to another group](#)

Managing groups of clients

In Symantec Endpoint Protection Manager, groups function as containers for the endpoints that run the client software. These endpoints can be either computers, or users. You organize the clients that have similar security needs into groups to make it easier to manage network security.

Symantec Endpoint Protection Manager contains the following default groups:

- The **My Company** group is the top-level, or parent, group. It contains a flat tree of child groups.

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

Note: You cannot rename or delete the default groups.

Table 9-1 Group management actions

Task	Description
Add groups	<p>See “How you can structure groups” on page 238.</p> <p>See “Adding a group” on page 239.</p>
Import existing groups	<p>If your organization already has an existing group structure, you can import the groups as organizational units.</p> <p>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.</p> <p>See “Importing existing groups and computers from an Active Directory or an LDAP server” on page 240.</p>
Disable inheritance for subgroups	<p>The subgroups inherit the same security settings from the parent group by default. You can disable inheritance.</p> <p>See “Disabling and enabling a group's inheritance” on page 247.</p>
Create locations within groups	<p>You can set up the clients to switch automatically to a different security policy if the physical location of the client changes.</p> <p>See “Managing locations for remote clients” on page 276.</p> <p>Some security settings are group-specific and some settings are location-specific. You can customize any settings that are location-specific.</p> <p>See “Configuring communication settings for a location” on page 285.</p>
Assign clients to groups before you install the client software	<p>You must apply the policy to the group for the policy to take effect.</p> <p>See “Assigning clients to groups before you install the client software” on page 246.</p>

Table 9-1 Group management actions (*continued*)

Task	Description
Manage security policies for groups	<p>You can create security policies based on the needs of each group. You can then assign different policies to different groups or locations.</p> <p>See “Adding a policy” on page 320.</p> <p>See “Assigning a policy to a group” on page 323.</p> <p>See “Performing the tasks that are common to all policies” on page 315.</p>
Perform group maintenance	<p>You can move groups for easier management and move clients between groups. You can also block clients from being added to a particular group.</p> <p>See “Moving a client computer to another group” on page 248.</p> <p>See “Blocking client computers from being added to groups” on page 248.</p>

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 9-2 Criteria for creating groups

Criterion	Description
Function	You can create groups based on the types of computers to be managed, such as laptops, desktops, and servers. Alternatively, you can create multiple groups that are based on usage type. For example, you can create a remote group for the client computers that travel and a local group for the client computers that remain in the office.
Role	You can create groups for department roles, such sales, engineering, finance, and marketing.
Geography	You can create groups based on the offices, cities, states, regions, or countries where the computers are located.

Table 9-2 Criteria for creating groups (*continued*)

Criterion	Description
Combination	<p>You can create groups based on a combination of criteria. For example, you can use the function and the role.</p> <p>You can add a parent group by role and add child subgroups by function, as in the following scenario:</p> <ul style="list-style-type: none"> ■ 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 315.

See [“Managing groups of clients”](#) on page 236.

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 238.

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.

Importing existing groups and computers from an Active Directory or an LDAP server

- 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 9-3](#) lists the tasks you should perform to import the group structure before you can manage them.

Table 9-3 Importing existing groups and computers

Step	Task	Description
Step 1	Connect Symantec Endpoint Protection Manager to your company's directory server	<p>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.</p> <p>See “About importing organizational units from the directory server” on page 241.</p> <p>See “Connecting Symantec Endpoint Protection Manager to a directory server” on page 242.</p> <p>See “Connecting to a directory server on a replicated site” on page 243.</p>
Step 2	Import either entire organizational units or specific computer accounts or user accounts	<p>You can either import the existing group structure, or import individual computer accounts or user accounts into the Symantec Endpoint Protection Manager groups that you create.</p> <p>See “Importing organizational units from a directory server” on page 244.</p> <p>If you want to use the group structure of Symantec Endpoint Protection Manager and not the directory server, import individual accounts.</p> <p>See “Searching for and importing specific accounts from a directory server” on page 245.</p>

Table 9-3 Importing existing groups and computers (*continued*)

Step	Task	Description
Step 3	Either keep imported computer or user accounts in their own group or copy imported accounts to existing groups	<p>After you import organizational units, you can do either of the following actions:</p> <ul style="list-style-type: none"> 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 239. <p>See “Assigning a policy to a group” on page 323.</p> <p>See “The types of security policies” on page 318.</p>
Step 4	Change the authentication method for administrator accounts (optional)	<p>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.</p> <p>See “Changing the authentication method for administrator accounts” on page 297.</p> <p>See “Best practices for testing whether a directory server authenticates an administrator account” on page 300.</p>

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 242.

See [“Importing existing groups and computers from an Active Directory or an LDAP server”](#) on page 240.

See [“Importing organizational units from a directory server”](#) on page 244.

See [“Searching for and importing specific accounts from a directory server”](#) on page 245.

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 244.

See [“Searching for and importing specific accounts from a directory server”](#) on page 245.

See [“Importing existing groups and computers from an Active Directory or an LDAP server”](#) on page 240.

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

Importing existing groups and computers from an Active Directory or an LDAP server

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 718.

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 242.

Importing organizational units from a directory server

When you import computer accounts or user accounts from an Active Directory or LDAP server, you import these accounts as organizational units. You can then apply a security policy to the organizational unit. You can also copy these accounts to an existing Symantec Endpoint Protection Manager group.

You can import the organizational unit as a subgroup of either the **My Company** group or a group you create, but not the **Default Group**. You cannot create groups as a subgroup of an organizational unit. You cannot place an organizational unit in more than one Symantec Endpoint Protection Manager group.

If you do not want to import all computer accounts or user accounts within a group, then you can select and import specific accounts.

See [“Searching for and importing specific accounts from a directory server”](#) on page 245.

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 242.
- 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 240.

See [“About importing organizational units from the directory server”](#) on page 241.

Searching for and importing specific accounts from a directory server

You can import specific computer accounts or user accounts rather than an entire group structure from a directory server into Symantec Endpoint Protection Manager groups. You should import specific accounts if you want to apply different security policies for the accounts in an organizational unit.

For example, you might want to maintain remote computers in one group. You would create a group for remote computers and assign a group policy that is tailored for remote computers in that group. You can then search for and import computers from the organizational unit directly to the remote group.

If you do not want to import specific accounts, then you can import all accounts within an organizational unit.

To search for and import specific accounts from a directory server

- 1 Connect to a directory server.

See [“Connecting Symantec Endpoint Protection Manager to a directory server”](#) on page 242.

- 2 In the console, click **Clients**.

- 3 On the **Clients** tab, under **Tasks**, click **Import Active Directory or LDAP Users**.

- 4 In the **Import Active Directory or LDAP Users** dialog box, select the server name in the **Directory Server** drop-down list.

The user name and password of the server automatically appears.

If **Only show users that are not added in any group** is checked, only those accounts appear that have not already been added.

- 5 Click **List Users**.

In the **LDAP Filter** field, you can also type an LDAP query to locate the names of accounts that you want to import.

For more information, click **Help**.

- 6 To select specific accounts, click **Add**, or click **Add All**.

- 7 Click **Close**.

See [“Importing organizational units from a directory server”](#) on page 244.

Assigning clients to groups before you install the client software

You can assign your clients to their groups before you install the client software. If you perform this task first, you can assign security policies to the client separately from the installation. In this case, the client does not receive the security policies from the group that is specified in the client installation package. Instead, the client is assigned to the group that you specified before installation.

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

See [“Switching a Windows client between user mode and computer mode”](#) on page 263.

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

See [“Blocking client computers from being added to groups”](#) on page 248.

To assign clients to groups before you install the client software

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

Disabling and enabling a group's inheritance

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

See [“Managing groups of clients”](#) on page 236.

To disable or enable a group's inheritance

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

You can select any group except the top-level group, My Company.

- 3 In the **group name** pane, on the **Policies** tab, do one of the following tasks:

- To disable inheritance, uncheck **Inherit policies and settings from parent group "group name"**.
- To enable inheritance, check **Inherit policies and settings from parent group "group name"**, and then click **Yes** when asked to proceed.

Blocking client computers from being added to groups

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

See [“Managing client installation packages”](#) on page 140.

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 248.

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 175.

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 236.

Managing clients

This chapter includes the following topics:

- [Managing client computers](#)
- [Viewing the protection status of clients and client computers](#)
- [Searching for the clients that do not have the client software installed](#)
- [Searching for information about client computers](#)
- [About enabling and disabling protection when you need to troubleshoot problems](#)
- [About commands that you can run on client computers](#)
- [Running commands on client computers from the console](#)
- [Ensuring that a client does not restart](#)
- [Switching a Windows client between user mode and computer mode](#)
- [Configuring a client to detect unmanaged devices](#)
- [About access to the client interface on Windows clients](#)
- [Locking and unlocking settings by changing the user control level](#)
- [Unlocking user interface settings on the client](#)
- [Collecting user information](#)
- [Password-protecting the client](#)

Managing client computers

[Table 10-1](#) lists the tasks you should perform with the computers after you install the client software.

Table 10-1 Tasks to manage client computers

Task	Description
<p>Check that the client software is installed on your computers</p>	<ul style="list-style-type: none"> ■ 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 254. ■ 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 265. ■ You can add a client to a group and install the client software later. See “About client installation methods” on page 115.
<p>Check whether the client is connected to the management server</p>	<p>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.</p> <p>See “How to determine whether the client is connected in the console” on page 167.</p> <p>See “How to determine whether the client computer is connected and protected” on page 169.</p> <p>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.</p> <p>See “Why do I need to replace the client-server communications file on the client computer?” on page 173.</p>
<p>Configure the connection between the client and the server</p>	<p>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.</p> <p>See “Managing the client-server connection” on page 165.</p> <p>You can troubleshoot any connection issues.</p> <p>See “Troubleshooting communication problems between the management server and the console or the database” on page 754.</p>

Table 10-1 Tasks to manage client computers (*continued*)

Task	Description
<p>Check that client computers have the right level of protection</p>	<ul style="list-style-type: none"> ■ You can view the status of each protection technology on your client computers. See “Viewing the protection status of clients and client computers” on page 253. See “How to determine whether the client is connected in the console” on page 167. ■ 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 593. ■ 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 255.
<p>Adjust the protection on client computers</p>	<p>If you decide that clients do not have the right level of protection, you can adjust the protection settings.</p> <ul style="list-style-type: none"> ■ 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 318. See “How Symantec Endpoint Protection uses layers to protect computers” on page 36. ■ You can temporarily disable protection on the client computers if you need to diagnose a problem or improve performance. See “About enabling and disabling protection when you need to troubleshoot problems” on page 256. See “Running commands on client computers from the console” on page 261. ■ You can require a password on the client. See “Password-protecting the client” on page 273.
<p>Move endpoints from one group to another to modify protection (optional)</p>	<p>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 248.</p> <p>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.</p>

Table 10-1 Tasks to manage client computers (*continued*)

Task	Description
Let users control computer protection (optional)	<p>You can specify the kind of control that users have over the protection on client computers.</p> <ul style="list-style-type: none"> ■ For Virus and Spyware Protection and Proactive Threat Protection, you can lock or unlock a check box to specify whether users can change individual settings. See “Locking and unlocking Virus and Spyware Protection policy settings” on page 330. ■ 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 “Locking and unlocking settings by changing the user control level” on page 267. ■ If users need full control of the client, you can install an unmanaged client. See “Why do I need to replace the client-server communications file on the client computer?” on page 173.
Remove the Symantec Endpoint Protection client software from decommissioned computers (optional)	<p>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.</p> <p>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.</p> <p>See “Uninstalling the Symantec Endpoint Protection client for Windows” on page 137.</p> <p>See “Uninstalling the Symantec Endpoint Protection client for Linux” on page 139.</p> <p>See “Purging obsolete clients from the database to make more licenses available” on page 104.</p>

Viewing the protection status of clients and client computers

You can view information about the real-time operational and protection status of the clients and the computers in your network.

You can view:

- A list of managed client computers that do not have the client installed. You can view the computer name, the domain name, and the name of the user who is logged on.

Searching for the clients that do not have the client software installed

- If the client is a virtual machine in a VMware infrastructure that uses a Security Virtual Appliance, the Security Virtual Appliance that the client is associated with.
- Which protections are enabled and disabled.
- Which client computers have the latest policies and definitions.
- The group's policy serial number and the client's version number.
- The information about the client computer's network components, such as the MAC address of the network card that the computer uses.
- The system information about the client computer, such as the amount of available disk space and the operating system version number.

After you know the status of a particular client, you can resolve any security issues on the client computers. You can resolve many issues by running commands on groups. For example, you can update content, or enable Auto-Protect.

Note: If you manage 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 [“How to determine whether the client is connected in the console”](#) on page 167.

See [“Running commands on client computers from the console”](#) on page 261.

See [“Searching for the clients that do not have the client software installed”](#) on page 254.

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 clients and client computers”](#) on page 253.

See [“How to determine whether the client is connected in the console”](#) on page 167.

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 272.

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 in 12.1.6, 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 clients and client computers”](#) on page 253.

About enabling and disabling protection when you need to troubleshoot problems

In general, you always want to keep the protection technologies enabled on a client computer.

You might need to temporarily disable either all the protection technologies or individual protection technologies if you have a problem with the client computer. For example, if an application does not run or does not run correctly, you might want to disable Network Threat Protection. If you still have the problem after you disable all protection technologies, completely uninstall the client. If the problem persists, you know that the problem is not due to Symantec Endpoint Protection.

Warning: Be sure to enable again any of the protections when you have completed your troubleshooting task to ensure that the computer remains protected.

[Table 10-2](#) describes the reasons why you might want to disable each protection technology.

Table 10-2 Purpose for disabling a protection technology

Protection technology	Purpose for disabling the protection technology
Virus and Spyware Protection	<p>If you disable this protection, you disable Auto-Protect only.</p> <p>Note: If you disable Auto-Protect, you also disable Download Insight, even if Download Insight is enabled. SONAR also cannot detect heuristic threats. SONAR detection of host file and system changes continues to function.</p> <p>The scheduled or startup scans still run if you or the user has configured them to do so.</p> <p>You might enable or disable Auto-Protect for the following reasons:</p> <ul style="list-style-type: none"> ■ Auto-Protect might block you from opening a document. For example, if you open a Microsoft Word that has a macro, Auto-Protect may not let you open it. If you know the document is safe, you can disable Auto-Protect. ■ Auto-Protect may warn you about a virus-like activity that you know is not the work of a virus. For example, you might get a warning when you install new computer applications. If you plan to install more applications and you want to avoid the warning, you can temporarily disable Auto-Protect. ■ Auto-Protect may interfere with Windows driver replacement. ■ Auto-Protect might slow down the client computer. <p>See “Running commands on client computers from the console” on page 261.</p> <p>If Auto-Protect causes a problem with an application, it is better to create an exception than to permanently disable the protection.</p> <p>See “Creating exceptions for Virus and Spyware scans” on page 498.</p>
Proactive Threat Protection	<p>You might want to disable Proactive Threat Protection for the following reasons:</p> <ul style="list-style-type: none"> ■ You see too many warnings about the threats that you know are not threats. ■ Proactive Threat Protection might slow down the client computer. <p>See “Adjusting SONAR settings on your client computers” on page 490.</p>

Table 10-2 Purpose for disabling a protection technology (*continued*)

Protection technology	Purpose for disabling the protection technology
Network Threat Protection	<p>You might want to disable Network Threat Protection for the following reasons:</p> <ul style="list-style-type: none"> ■ You install an application that might cause the firewall to block it. ■ The firewall or the Intrusion Prevention System causes network connectivity-related issues. ■ The firewall might slow down the client computer. ■ You cannot open an application. <p>If you are not sure that Network Threat Protection causes the problem, you might need to disable all the protection technologies.</p> <p>You can configure Network Threat Protection so that users cannot enable or disable it. You can also set the following limits for when and how long the protection is disabled:</p> <ul style="list-style-type: none"> ■ Whether the client allows either all traffic or all outbound traffic only. ■ The length of time the protection is disabled. ■ How many times you can disable protection before you restart the client. <p>See “Enabling or disabling network intrusion prevention or browser intrusion prevention” on page 386.</p> <p>See “Unlocking user interface settings on the client” on page 270.</p>
Tamper Protection	<p>Typically, you should keep Tamper Protection enabled.</p> <p>You might want to disable Tamper Protection temporarily if you get an extensive number of false positive detections. For example, some third-party applications might make the changes that inadvertently try to modify Symantec settings or processes. If you are sure that an application is safe, you can create a Tamper Protection exception for the application.</p> <p>See “Changing Tamper Protection settings” on page 494.</p>

About commands that you can run on client computers

You can run commands remotely on individual clients or an entire group from the console.

You can enable and disable protection to troubleshoot problems on the client computer.

See [“About enabling and disabling protection when you need to troubleshoot problems”](#) on page 256.

Table 10-3 Commands that you can run on client computers

Commands	Description
Scan	<p>Runs on-demand scan on the client computers.</p> <p>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.</p> <p>See “Running on-demand scans on client computers” on page 426.</p>
Update Content	<p>Updates content on clients by initiating a LiveUpdate session on the client computers. The clients receive the latest content from Symantec LiveUpdate.</p> <p>See “Configuring the LiveUpdate download schedule for Symantec Endpoint Protection Manager” on page 192.</p>
Update Content and Scan	<p>Updates content by initiating a LiveUpdate session and runs an on-demand scan on client computers.</p>
Start Power Eraser Analysis	<p>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.</p> <p>Note: Mac and Linux client computers do not process this command.</p> <p>See “Starting Power Eraser analysis from Symantec Endpoint Protection Manager” on page 770.</p>

Table 10-3 Commands that you can run on client computers (*continued*)

Commands	Description
Restart Client Computers	<p>Restarts the client computers.</p> <p>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.</p> <p>Note: Restart options apply only to Windows client computers. Mac client computers always perform a hard restart. Linux client computers ignore this command.</p> <p>See “Restarting the client computers from Symantec Endpoint Protection Manager” on page 129.</p> <p>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.</p> <p>See “Ensuring that a client does not restart” on page 263.</p>
Enable Auto-Protect	<p>Enables Auto-Protect for the file system on the client computers.</p> <p>By default, Auto-Protect for the file system is enabled. You might need to enable Auto-Protect from the console if you have allowed users to change the setting or if you disable Auto-Protect. You can lock the setting so that users on client computers cannot disable Auto-Protect.</p> <p>See “Customizing Auto-Protect for Windows clients” on page 464.</p> <p>See “Customizing Auto-Protect for Mac clients” on page 465.</p> <p>If you want to enable or disable Auto-Protect for email, you must include the setting in the Virus and Spyware Protection policy.</p>
Enable Network Threat Protection and Disable Network Threat Protection	<p>Enables or disables the firewall and enables intrusion prevention on the client computers.</p> <p>Note: Linux client computers do not process this command.</p> <p>See “Managing firewall protection” on page 336.</p>
Enable Download Insight and Disable Download Insight	<p>Enables or disables Download Insight on the client computers.</p> <p>Note: Mac and Linux client computers do not process this command.</p> <p>See “Managing Download Insight detections” on page 432.</p>

Table 10-3 Commands that you can run on client computers (*continued*)

Commands	Description
Delete From Quarantine	<p>Deletes all files from Quarantine.</p> <p>Note: You can access this command by clicking Admin > Admin > Add an Administrator > Access Rights.</p>
Collect file fingerprint list	<p>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.</p> <p>Note: Mac and Linux client computers do not process this command.</p>

You can configure a limited administrator to have rights to some or none of these commands.

See [“Running commands on client computers from the console”](#) on page 261.

See [“Configuring the access rights for a limited administrator”](#) on page 296.

See [“Management features based on platform”](#) on page 776.

Running commands on client computers from the console

You can run commands at any time on a client or a group, such as starting 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 [“About commands that you can run on client computers”](#) on page 258.

You run these commands from the following locations:

- The **Clients** page.
- The **Computer Status** log.

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:
 - In the left pane, under **Clients**, right-click the group for which you want to run the command, and then click **Run a command on the group > command**
 - In the right pane, on the **Clients** tab, right-click the computers or users 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**.

To cancel a scan in progress, click **Cancel All Scans** from the command list.

- 3 If there are settings choices for the command that you selected, a message appears where you can configure the appropriate settings.
- 4 When you have finished configuration, click **Yes** or **OK**.
- 5 In the command confirmation message box that appears, click **Yes**.
- 6 In the **Message** dialog box, click **OK**.

If the command is not queued successfully, you may need to repeat this procedure. You can check to see if the server is down. If the console has lost connectivity with the server, you can log off the console and then log back on to see if that helps.

To view 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 are only installed in computer mode.

Switching a Windows client between user mode and computer mode

Mode	Description
Computer mode	<p>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.</p> <p>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.</p> <p>Clients that you add in computer mode can be enabled as unmanaged detectors, and used to detect unauthorized devices.</p> <p>See "Configuring a client to detect unmanaged devices" on page 265.</p>
User mode	<p>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.</p> <p>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.</p> <p>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.</p> <p>See "Importing existing groups and computers from an Active Directory or an LDAP server" on page 240.</p>

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.

See [“Assigning clients to groups before you install the client software”](#) on page 246.

Configuring a client to detect unmanaged devices

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

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

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

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

- Enable Network Threat Protection.
See [“Running commands on client computers from the console”](#) on page 261.
- Switch the client to computer mode.
See [“Switching a Windows client between user mode and computer mode”](#) on page 263.

- 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.

About access to the client interface on Windows clients

You can determine the level of interaction that you want users to have on the Symantec Endpoint Protection Windows client. Choose which features are available for users to configure. For example, you can control the number of notifications that appear and limit users' ability to create firewall rules and virus and spyware scans. You can also give users full access to the user interface.

The features that users can customize for the user interface are called managed settings. The user does not have access to all the client features, such as password protection.

To determine the level of user interaction, you can customize the user interface in the following ways:

- For virus and spyware settings, you can lock or unlock the settings. See [“Locking and unlocking Virus and Spyware Protection policy settings”](#) on page 330.
- For firewall settings, intrusion prevention settings, and for some client user interface settings, you can set the user control level and configure the associated settings. See [“Unlocking user interface settings on the client”](#) on page 270. See [“Locking and unlocking settings by changing the user control level”](#) on page 267. See [“Configuring firewall settings for mixed control”](#) on page 344.
- You can password-protect the client. See [“Password-protecting the client”](#) on page 273.

Locking and unlocking settings by changing the user control level

You can lock some Virus and Spyware Protection policy settings so that users cannot change them on the Windows client.

However, to lock other protection settings and the client user interface settings, you use a different method. To determine which settings are available for users to change, you specify the user control level. The user control level determines whether the client can be completely invisible, display a partial set of features, or display a full user interface.

In releases earlier than 12.1, a change from client control to server control causes all settings, regardless of their control level status, to revert to their server control default values the next time policies are distributed to clients. In 12.1 and later, locks are in effect in all control modes. Unlocked settings behave in server control and client control modes in the following ways:

- In Server Control, changes can be made to unlocked settings, but they are overwritten when the next policy is applied.
- In Client Control, client-modified settings take precedence over server settings. They are not overwritten when the new policy is applied, unless the setting has been locked in the new policy.

Table 10-4 User control levels

User control level	Description
Server control	<p>Gives the users the least control over the client. Server control locks the managed settings so that users cannot configure them.</p> <p>Server control has the following characteristics:</p> <ul style="list-style-type: none"> ■ Users cannot configure or enable firewall rules, application-specific settings, firewall settings, intrusion prevention settings, or Network Threat Protection and Client Management logs. You configure all the firewall rules and security settings for the client in Symantec Endpoint Protection Manager. ■ Users can view logs, the client's traffic history, and the list of applications that the client runs. ■ You can configure certain user interface settings and firewall notifications to appear or not appear on the client. For example, you can hide the client user interface. <p>The settings that you set to server control either appear dimmed or are not visible in the client user interface.</p> <p>When you create a new location, the location is automatically set to server control.</p>
Client control	<p>Gives the users the most control over the client. Client control unlocks the managed settings so that users can configure them.</p> <p>Client control has the following characteristics:</p> <ul style="list-style-type: none"> ■ Users can configure or enable firewall rules, application-specific settings, firewall notifications, firewall settings, intrusion prevention settings, and client user interface settings. ■ The client ignores the firewall rules that you configure for the client. <p>You can give client control to the client computers that employees use in a remote location or a home location.</p>

Table 10-4 User control levels (*continued*)

User control level	Description
Mixed control	<p>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. In client control, only the user can enable or disable the setting. In server control, only you can enable or disable the setting.</p> <p>If you assign an option to server control, you then configure the setting in the corresponding page or dialog box in the Symantec Endpoint Protection Manager console. For example, you can enable the firewall settings in the Firewall policy. You can configure the logs in the Client Log Settings dialog box on the Policies tab of the Clients page.</p> <p>Mixed control has the following characteristics:</p> <ul style="list-style-type: none"> ■ Users can configure some of the settings for the firewall, Intrusion Prevention, and the client user interface. ■ You can configure the firewall rules, which may or may not override the rules that users configure. The position of the server rules in the Rules list of the firewall policy determines whether server rules override client rules. ■ You can specify certain settings to be available or not available on the client for users to enable and configure. These settings include the Network Threat Protection logs, Client Management logs, firewall settings, intrusion prevention settings, and some user interface settings. ■ You can configure Virus and Spyware Protection settings to override the setting on the client, even if the setting is unlocked. For example, if you unlock the Auto-Protect feature and the user disables it, you can enable Auto-Protect. <p>The settings that you set to client control are available to the user. The settings that you set to server control either appear dimmed or are not visible in the client user interface.</p>

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.

Note: Clients that run in client control or mixed control switch to server control when the server applies a Quarantine policy.

To change the user control level

- 1 In the console, click **Clients**.
- 2 Under **View Clients**, select the group whose location you want to modify.
- 3 Click the **Policies** tab.

- 4 Under **Location-specific Policies and Settings**, under the location you want to modify, expand **Location-specific Settings**.
- 5 To the right of **Client User Interface Control Settings**, click **Tasks > Edit Settings**.
- 6 In the **Client User Interface Control Settings** dialog box, do one of the following options:
 - Click **Server control**, and then click **Customize**. Configure any of the settings, and then click **OK**.
 - Click **Client control**.
 - Click **Mixed control**, and then click **Customize**. Configure any of the settings, and then click **OK**.
- 7 Click **OK**.

See [“Unlocking user interface settings on the client”](#) on page 270.

See [“Locking and unlocking Virus and Spyware Protection policy settings”](#) on page 330.

Unlocking user interface settings on the client

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 [“Locking and unlocking settings by changing the user control level”](#) on page 267.
- 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 and intrusion prevention settings, configure them in the Firewall policy and Intrusion Prevention policy.
 See [“Automatically allowing communications for essential network services”](#) on page 343.
 See [“Detecting potential attacks and spoofing attempts”](#) on page 346.
 See [“Enabling or disabling network intrusion prevention or browser intrusion prevention”](#) on page 386.
- 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 [“Locking and unlocking settings by changing the user control level”](#) on page 267.
- 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**.

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 140.

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 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.
- Uninstall the client.
- Import and export the security policy.

You can modify the password protection settings for any child group that does not inherit its settings from a parent.

See [“About access to the client interface on Windows clients”](#) on page 266.

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 Settings**.
- 4 On the **Password Settings** tab, check any or all of the check boxes.
- 5 In the **Password** and **Confirm password** text boxes, type the same password.

The password is limited to 15 characters or less.
- 6 Click **OK**.

Managing remote clients

This chapter includes the following topics:

- [Managing remote clients](#)
- [Managing locations for remote clients](#)
- [Enabling location awareness for a client](#)
- [Adding a location to a group](#)
- [Changing a default location](#)
- [Setting up Scenario One location awareness conditions](#)
- [Setting up Scenario Two location awareness conditions](#)
- [Configuring communication settings for a location](#)
- [About strengthening your security policies for remote clients](#)
- [About turning on notifications for remote clients](#)
- [About customizing log management settings for remote clients](#)
- [About monitoring remote clients](#)

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 11-1 Managing remote clients

Task	Description
Set up groups based on assessment of security risk	See " Managing groups of clients " on page 236.
Set up locations for groups of remote clients	See " Managing locations for remote clients " on page 276.
Configure communication settings for locations	See " Configuring communication settings for a location " on page 285.
Strengthen your security policies	See " About strengthening your security policies for remote clients " on page 286.
Turn on client notifications	See " About turning on notifications for remote clients " on page 288.
Customize client log management settings	See " About customizing log management settings for remote clients " on page 289.
Monitor remote clients	See " About monitoring remote clients " on page 289.

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 11-2 Location awareness tasks that you can perform

Tasks	Description
Plan locations	<p>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.</p> <p>See “Managing groups of clients” on page 236.</p> <p>You may find the following examples helpful:</p> <p>See “Setting up Scenario One location awareness conditions” on page 281.</p> <p>See “Setting up Scenario Two location awareness conditions” on page 283.</p>
Enable location awareness	<p>To control the policies that are assigned to clients contingent on the location from which the clients connect, you can enable location awareness.</p> <p>See “Enabling location awareness for a client” on page 278.</p>
Add locations	<p>You can add locations to groups.</p> <p>See “Adding a location to a group” on page 279.</p>
Assign default locations	<p>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.</p> <p>The default location is used if one of the following cases occurs:</p> <ul style="list-style-type: none"> ■ 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. <p>See “Changing a default location” on page 280.</p>

Table 11-2 Location awareness tasks that you can perform (*continued*)

Tasks	Description
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 285.

See the knowledge base article [Best Practices for Symantec Endpoint Protection Location Awareness](#).

See [“Configuring communication settings for a location”](#) on page 285.

See [“Managing remote clients”](#) on page 274.

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 276.

See [“Adding a location to a group”](#) on page 279.

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 236.
- See [“About strengthening your security policies for remote clients”](#) on page 286.

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 276.

Setting up Scenario One location awareness conditions

If you have remote clients, in the simplest case, it is a common practice to use the My Company group and three locations. This is Scenario One.

To manage the security of the clients in this scenario, you can create the following locations under the My Company group to use:

- Office clients that log on in the office.
- The remote clients that log on to the corporate network remotely over a VPN.
- The remote clients that log on to the Internet remotely, but not over a VPN.

Because the remote location with no VPN connection is the least secure, it has the most secure policies. It is a best practice to always make this location the default location.

Note: If you turn off My Company group inheritance and then you add groups, the added groups do not inherit the locations that you set up for the My Company group.

The following suggestions represent the best practices for Scenario One.

To set up the office location for the clients located in the office

- 1 On the **Clients** page, select the group that you want to add a location for.
- 2 On the **Policies** tab, under **Tasks**, click **Add Location**.
- 3 In the **Add Location Wizard**, click **Next**.
- 4 Type a name for the location and optionally, add a description of it, and then click **Next**.
- 5 In the list box, click **Client can connect to management server** from the list, and then click **Next**.

- 6 Click **Finish**, and then click **OK**.
- 7 Under **Tasks**, click **Manage Locations**, and then select the location you created.
- 8 Click **Add**, and then click **Criteria with AND relationship**.
- 9 In the **Specify Location Criteria** dialog box, from the **Type** list, click **Network Connection Type**.
- 10 Click **If the client computer does not use the network connection type specified below**.
- 11 In the bottom list box, select the name of the VPN client that your organization uses, and then click **OK**.
- 12 Click **OK** to exit the **Manage Locations** dialog box.

To set up the remote location for the clients logging in over a VPN

- 1 On the **Clients** page, select the group that you want to add a location for.
- 2 On the **Policies** tab, under **Tasks**, click **Add Location**.
- 3 In the **Add Location Wizard**, click **Next**.
- 4 Type a name for the location and optionally, add a description of it, and then click **Next**.
- 5 In the list box, click **Network connection type**.
- 6 In the **Connection Type** list box, select the name of the VPN client that your organization uses, and then click **Next**.
- 7 Click **Finish**.
- 8 Click **OK**.

To set up the remote location for the clients not logging on over a VPN

- 1 On the **Clients** page, select the group that you want to add a location for.
- 2 On the **Policies** tab, under **Tasks**, click **Add Location**.
- 3 In the **Add Location Wizard**, click **Next**.
- 4 Type a name for the location, optionally add a description of it, and then click **Next**.
- 5 In the list box, leave **No specific condition**, and then click **Next**.

By using these settings, this location's policies, which should be the strictest and most secure, are used as the default location policies.

- 6 Click **Finish**, and then click **OK**.

See [“Setting up Scenario Two location awareness conditions”](#) on page 283.

See [“Managing remote clients”](#) on page 274.

Setting up Scenario Two location awareness conditions

In Scenario Two, you use the same two remote locations as specified in Scenario One and two office locations, for a total of four locations.

You would add the following office locations:

- Clients in the office that log on over an Ethernet connection.
- Clients in the office that log on over a wireless connection.

It simplifies management to leave all clients under the default server control mode. If you want granular control over what your users can and cannot do, an experienced administrator can use mixed control. A mixed control setting gives the end user some control over security settings, but you can override their changes, if necessary. Client control allows users a wider latitude in what they can do and so constitutes a greater risk to network security.

We suggest that you use client control only in the following situations:

- If your users are knowledgeable about computer security.
- If you have a compelling reason to use it.

Note: You may have some clients that use Ethernet connections in the office while other clients in the office use wireless connections. For this reason, you set the last condition in the procedure for wireless clients in the office. This condition lets you create an Ethernet location Firewall policy rule to block all wireless traffic when both kinds of connections are used simultaneously.

To set up the office location for the clients that are logged on over Ethernet

- 1 On the **Clients** page, select the group that you want to add a location for.
- 2 Under **Tasks**, click **Add Location**.
- 3 In the **Add Location Wizard**, click **Next**.
- 4 Type a name for the location, optionally add a description of it, and then click **Next**.
- 5 In the list box, select **Client can connect to management server**, and then click **Next**.
- 6 Click **Finish**.

- 7 Click **OK**.
- 8 Under **Tasks**, click **Manage Locations**, and then select the location you created.
- 9 Beside **Switch to this location when**, click **Add**, and then select **Criteria with AND relationship**.
- 10 In the **Specify Location Criteria** dialog box, from the **Type** list, click **Network Connection Type**.
- 11 Click **If the client computer does not use the network connection type specified below**.
- 12 In the bottom list box, select the name of the VPN client that your organization uses, and then click **OK**.
- 13 Click **Add** and then click **Criteria with AND relationship**.
- 14 In the **Specify Location Criteria** dialog box, from the **Type** list, click **Network Connection Type**.
- 15 Click **If the client computer uses the network connection type specified below**.
- 16 In the bottom list box, select **Ethernet**, and then click **OK**.
- 17 Click **OK** to exit the Manage Locations dialog box.

To set up the office location for the clients that are logged on over a wireless connection

- 1 On the **Clients** page, select the group that you want to add a location for.
- 2 Under **Tasks**, click **Add Location**.
- 3 In the **Add Location Wizard**, click **Next**.
- 4 Type a name for the location, optionally add a description of it, and then click **Next**.
- 5 In the list box, click **Client can connect to management server**, and then click **Next**.
- 6 Click **Finish**.
- 7 Click **OK**.
- 8 Under **Tasks**, click **Manage Locations**, and then select the location that you created.
- 9 Beside **Switch to this location when**, click **Add**, and then click **Criteria with AND relationship**.

- 10 In the **Specify Location Criteria** dialog box, from the **Type** list, click **Network Connection Type**.
 - 11 Click **If the client computer does not use the network connection type specified below**.
 - 12 In the bottom list box, select the name of the VPN client that your organization uses, and then click **OK**.
 - 13 Click **Add**, and then click **Criteria with AND relationship**.
 - 14 In the **Specify Location Criteria** dialog box, from the **Type** list, click **Network Connection Type**.
 - 15 Click **If the client computer does not use the network connection type specified below**.
 - 16 In the bottom list box, click **Ethernet**, and then click **OK**.
 - 17 Click **Add**, and then click **Criteria with AND relationship**.
 - 18 In the **Specify Location Criteria** dialog box, from the **Type** list, click **Network Connection Type**.
 - 19 Click **If the client computer uses the network connection type specified below**.
 - 20 In the bottom list box, click **Wireless**, and then click **OK**.
 - 21 Click **OK** to exit the **Manage Locations** dialog box.
- See [“Setting up Scenario One location awareness conditions”](#) on page 281.
- See [“Managing remote clients”](#) on page 274.

Configuring communication settings for a location

By default, you configure communication settings between the management server and the client at the level of the group. However, you can also configure these settings for individual locations in a group. For example, you can use a separate management server for a location where the client computers connect through the VPN. To minimize the number of clients that connect to the management server at the same time, you can specify a different heartbeat for each location.

You can configure the following communication settings for locations:

- The control mode in which the clients run.
- The management server list that the clients use.
- The download mode in which the clients run.

- Whether to collect a list of all the applications that are executed on clients and send the list to the management server.
- The heartbeat interval that clients use for downloads.
- Whether the management server randomizes content downloads from the default management server or a Group Update Provider.

Note: Only some of these settings can be configured for Mac clients.

To configure communication settings for a location

- 1 In the console, click **Clients**.
- 2 On the **Clients** page, select a group.
- 3 On the **Policies** tab, under **Location-specific Policies and Settings**, under a location, expand **Location-specific Settings**.
- 4 To the right of **Communications Settings**, click **Tasks**, and then uncheck **Use Group Communications Settings**.
- 5 Click **Tasks** again, and then click **Edit Settings**.
- 6 In the **Communications Settings for *location name*** dialog box, modify the settings for the specified location only.
- 7 Click **OK**.

See [“Configuring push mode or pull mode to update client policies and content”](#) on page 170.

See [“Managing locations for remote clients”](#) on page 276.

See [“Managing groups of clients”](#) on page 236.

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 274.

Best practices for Firewall policy settings

[Table 11-3](#) describes scenarios and best-practice recommendations.

Table 11-3 Firewall policy best practices

Scenario	Recommendation
Remote location where users log on without a VPN	<ul style="list-style-type: none"> ■ Assign the strictest security policies to clients that log on remotely without using a VPN. ■ Enable NetBIOS protection. <p>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.</p> <ul style="list-style-type: none"> ■ 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	<ul style="list-style-type: none"> ■ 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. <p>Note: You need to make all of these changes if you want to avoid the possibility of split tunneling through the VPN.</p>
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 339.

See [“Automatically allowing communications for essential network services”](#) on page 343.

LiveUpdate policy settings for clients in different locations

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

For a remote location where users log in without a VPN, we suggest the following best practices:

- Change the LiveUpdate policy setting to use the default Symantec LiveUpdate server. This setting allows the remote clients to update any time they connect to the Internet.
- Change the LiveUpdate Schedule frequency setting to one hour to make it more likely that clients update their protection when they connect to the Internet.

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

See [“Managing remote clients”](#) on page 274.

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 274.

About customizing log management settings for remote clients

You may want to customize the log management settings for remote clients. Customization can be especially useful if clients are offline for several days.

The following settings can help reduce bandwidth and the load on your management servers:

- Clients do not upload their logs to the management server.
- Clients upload only the client security logs.
- Filter log events to upload only specified events.
Suggested events to upload include definition updates, or side effect repair failures.
- Make the log retention time longer.
Longer retention times let you review more antivirus and antispyware event data.

Note: Some client log settings are specific to a group. Location-specific log settings are part of a Virus and Spyware Protection policy. Depending on the log settings that you want to customize, you may need to use groups instead of locations to manage your remote clients.

See [“Viewing logs”](#) on page 613.

About monitoring remote clients

Notifications and logs are essential to maintain a secure environment. In general, you should monitor your remote clients in the same way that you monitor your other clients. You should always check to see that your protections are up to date and that your network is not currently under attack. If your network is under attack, then you want to find out who is behind the attack and how they attacked.

Your Home page preference settings determine the time period for which Symantec Endpoint Protection Manager displays data. By default, the data on the Home page represents only the clients that connected in the past 12 hours. If you have many clients that are frequently offline, your best monitoring option is to go to the logs and reports. In the logs and reports, you can filter the data to include offline clients.

Even if you restrict some of the client log data that mobile clients upload, you can check the following displays.

Table 11-4 Displays to monitor remote client security

Display	Description
Home > Endpoint Status	<p>Displays whether the content is up to date or to see if any of the protections are turned off.</p> <p>You can check the following status conditions:</p> <ul style="list-style-type: none"> ■ Content dates and version numbers ■ Client connections ■ Enabled and disabled protections <p>You can click Details to see the status for each client.</p>
Home > Security Status	<p>Displays the system security overview. View the Virus and Risks Activity Summary to see if your network is under attack.</p> <p>You can click Details to see the status for each security protection technology.</p>
Home > Virus and Risks Activity Summary	<p>Displays the detected virus and risk activity, and the actions taken, such as cleaned, blocked, or quarantined.</p>
Monitors > Summary Type > Network Threat Protection	<p>Displays the information about attack types and sources.</p>

See [“Managing remote clients”](#) on page 274.

Managing administrator accounts and passwords

This chapter includes the following topics:

- [Managing administrator accounts](#)
- [About administrator account roles and access rights](#)
- [Adding an administrator account](#)
- [Configuring the access rights for a limited administrator](#)
- [Changing the authentication method for administrator accounts](#)
- [Best practices for testing whether a directory server authenticates an administrator account](#)
- [Changing the password for an administrator account](#)
- [Resetting a forgotten Symantec Endpoint Protection Manager password](#)
- [Enabling Symantec Endpoint Protection Manager logon passwords to never expire](#)

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 12-1 Account administration

Task	Description
Decide whether to add multiple domains	<p>Decide whether to add domains.</p> <p>See “About domains” on page 309.</p> <p>See “Adding a domain” on page 311.</p> <p>See “Switching to the current domain” on page 311.</p>
Add administrator accounts	<p>Add accounts for administrators who need access to the Symantec Endpoint Protection Manager console.</p> <ul style="list-style-type: none"> ■ Learn about the administrator account roles that are available. See “About administrator account roles and access rights” on page 293. ■ Create the types of administrator accounts that you need. See “Adding an administrator account” on page 295. See “Configuring the access rights for a limited administrator” on page 296. ■ Change the method that is used to authenticate administrator accounts (optional). By default, the Symantec Endpoint Protection Manager database authenticates the administrator’s credentials. You can also use RSA SecurID or an LDAP server or a Microsoft Active Directory Server for authentication. See “Changing the authentication method for administrator accounts” on page 297.
Unlock or lock an administrator account	<p>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.</p> <p>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.</p> <p>See “Configuring an administrator’s account to lock after too many logon attempts” on page 84.</p>

Table 12-1 Account administration (*continued*)

Task	Description
Change and reset lost passwords	<ul style="list-style-type: none"> ■ Change the password for your account or another administrator's account. See "Changing the password for an administrator account" on page 305. ■ 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 "Displaying the Forgot your password? link so that administrators can reset lost passwords" on page 307. ■ 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 82. ■ 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 82.
Configure logon options for Symantec Endpoint Protection Manager	<p>You can configure the following logon options for each type of administrator:</p> <ul style="list-style-type: none"> ■ 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 82. ■ 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 83. ■ Changing how long an administrator can stay logged on to the management server. See "Changing the time period for staying logged on to the console" on page 85.

See ["Logging on to the Symantec Endpoint Protection Manager console"](#) on page 78.

About administrator account roles and access rights

When you install the Symantec Endpoint Protection Manager, a default system administrator account is created, called `admin`. The system administrator account gives an administrator access to all the features in Symantec Endpoint Protection Manager.

To help you manage security, you can add additional system administrator accounts, domain administrator accounts, and limited administrator accounts. Domain administrators and limited administrators have access to a subset of Symantec Endpoint Protection Manager features.

You choose which accounts you need based on the types of roles and access rights you need in your company. For example, a large company may use the following types of roles:

- An administrator who installs the management server and the client installation packages. After the product is installed, an administrator in charge of operations takes over. These administrators are most likely system administrators.
- An operations administrator maintains the servers, databases, and installs patches. If you have a single domain, the operations administrator could be a domain administrator who is fully authorized to manage sites.
- An antivirus administrator, who creates and maintains the Virus and Spyware 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 12-2 describes the account type and the access rights that each role has.

Table 12-2 Administrator roles and responsibilities

Administrator role	Responsibilities
System administrator	<p>System administrators can log on to the Symantec Endpoint Protection Manager console with complete, unrestricted access to all features and tasks.</p> <p>A system administrator can create and manage other system administrator accounts, domain administrator accounts, and limited administrator accounts.</p> <p>A system administrator can perform the following tasks:</p> <ul style="list-style-type: none"> ■ Manage all domains. ■ Administer licenses. ■ View and manage all console settings. ■ Manage the databases and management servers.

Table 12-2 Administrator roles and responsibilities (*continued*)

Administrator role	Responsibilities
Administrator	<p>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.</p> <p>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.</p> <p>A domain administrator can perform the following tasks:</p> <ul style="list-style-type: none"> ■ Create and manage administrator accounts and limited administrator accounts within a single domain. Domain administrators cannot modify their own site rights. System administrators must perform this function. ■ Run reports, manage sites, and reset passwords. You must explicitly configure reporting rights to groups that are migrated from Symantec AntiVirus 10.x. ■ Cannot administer licenses. Only system administrators can administer licenses. <p>See “About domains” on page 309.</p>
Limited administrator	<p>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.</p> <p>Parts of the management server user interface are not available to limited administrators when you restrict access rights. For example:</p> <ul style="list-style-type: none"> ■ 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. <p>See “Configuring the access rights for a limited administrator” on page 296.</p>

See [“Managing administrator accounts”](#) on page 291.

See [“Adding an administrator account”](#) on page 295.

Adding an administrator account

As a system administrator, you can add another system administrator, administrator, or limited administrator. As an administrator within a domain, you can add other administrators with access rights equal to or less restrictive than your own. Administrators can add limited administrators and configure their access rights.

To add an administrator account

- 1 In the console, click **Admin**.
- 2 On the **Admin** page, click **Administrators**.
- 3 Under **Tasks**, click **Add an administrator**.
- 4 In the **Add Administrator** dialog box, on the **General** tab, enter the user name and email address.
- 5 On the **Access Rights** and **Authentication** tabs, specify the administrator role, access rights, and authentication method.

See [“About administrator account roles and access rights”](#) on page 293.

See [“Changing the authentication method for administrator accounts”](#) on page 297.

Click **Help** for more information.
- 6 Click **OK**.

See [“Managing administrator accounts”](#) on page 291.

Configuring the access rights for a limited administrator

If you add an account for a limited administrator, you must also specify the administrator's access rights. Limited administrator accounts that are not granted any access rights are created in a disabled state and the limited administrator will not be able to log on to the management server.

To configure the access rights for a limited administrator

- 1 In the console, click **Admin**.
- 2 On the **Admin** page, click **Administrators**.
- 3 Select the limited administrator.

You can also configure the access rights when you create a limited administrator account.

See [“Adding an administrator account”](#) on page 295.
- 4 Under **Tasks**, click **Edit Administrator**.
- 5 On the **Access Rights** tab, check an option, and then click the corresponding button to set the access rights. Click **Help** for more information.

6 If you want to authorize the limited administrator to create only non-shared policies for a location, check **Only allow location-specific policy editing**.

7 Click **OK**.

See [“About administrator account roles and access rights”](#) on page 293.

See [“Managing administrator accounts”](#) on page 291.

Changing the authentication method for administrator accounts

After you add an administrator account, the user name and password are stored in the Symantec Endpoint Protection Manager database. When the administrator logs on to the management server, the management server verifies with the database that the user name and password are correct. However, if your company uses a third-party server to authenticate existing user names and passwords, you can configure Symantec Endpoint Protection Manager to authenticate with the server.

[Table 12-3](#) displays the authentication methods the management server can use to authenticate administrator accounts.

Table 12-3 Authentication methods

Symantec Endpoint Protection Manager authentication (default)	<p>Authenticates the administrators with the administrator's credentials that are stored in the Symantec Endpoint Protection Manager database.</p> <p>You can display the Password never expires option so that an administrator's account does not expire.</p> <p>See “Enabling Symantec Endpoint Protection Manager logon passwords to never expire” on page 308.</p>
RSA SecurID authentication	Authenticates the administrators by using RSA SecurID token (not software RSA tokens), RSA SecurID card, or RSA keypad card (not RSA smart cards).
Directory server authentication	Authenticates the administrators with an LDAP server or the Microsoft Active Directory server.

For the third-party authentication methods, Symantec Endpoint Protection Manager has an entry in the database for the administrator account, but the third-party server validates the user name and password.

To change the authentication method for administrator accounts

1 Add an administrator account.

See [“Adding an administrator account”](#) on page 295.

2 On the **Authentication** tab, select the authentication method.

- To authenticate administrators who use an RSA SecurID mechanism, first install the RSA ACE server and enable encrypted authentication for RSA SecurID.

See [“Configuring the management server to authenticate administrators who use RSA SecurID to log on”](#) on page 298.

See [“Authenticating administrators who use RSA SecurID to log on to the management server”](#) on page 300.

- 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.

You can check whether the directory server authenticates the account name by clicking **Test Account**.

See [“Connecting Symantec Endpoint Protection Manager to a directory server”](#) on page 242.

See [“Best practices for testing whether a directory server authenticates an administrator account”](#) on page 300.

3 Click **OK**.

4 In the **Confirm Change** dialog box, type the password that you use to log on to Symantec Endpoint Protection Manager, and then click **OK**.

When you switch between authentication methods, you must type the administrator account's password.

Configuring the management server to authenticate administrators who use RSA SecurID to log on

If your corporate network includes an RSA server, you need to install the software for an RSA ACE Agent on the computer on which you installed Symantec Endpoint Protection Manager and configure it as a SecurID Authentication client.

To configure the management server to authenticate administrators who use RSA SecurID to log on

- 1 Install the software for the RSA ACE Agent on the same computer on which you installed the management server. You can install the software by running the Windows .msi file from the RSA Authentication Agent installation file.
- 2 Copy the nodesecret.rec, sdconf.rec, and agent_nsload.exe files from the RSA ACE server to the computer on which you installed the management server.
- 3 At the command prompt, type the following command:


```
agent_nsload -f nodesecret.rec -p password
```

 where *password* is the password for the nodesecret file.
- 4 In the console, click **Admin**, and then click **Servers**.
- 5 Under **Servers**, select the management server to which you want to connect an RSA server.
- 6 Under **Tasks**, click **Configure SecurID authentication**.
- 7 In the **Welcome to the Configure SecurID Authentication Wizard** panel, click **Next**.
- 8 In the **Qualification** panel of the **Configure SecurID Authentication Wizard** panel, read the prerequisites so that you can meet all the requirements.
- 9 Click **Next**.
- 10 In the **Upload RSA File** panel of the **Configure SecurID Authentication Wizard** panel, browse for the folder in which the sdconf.rec file resides.
 You can also type the path name.
- 11 Click **Next**.
- 12 Click **Test** to test your configuration.
- 13 In the **Test Configuration** dialog box, type the user name and password for your SecurID, and then click **Test**.
 It now authenticates successfully.

See [“Authenticating administrators who use RSA SecurID to log on to the management server”](#) on page 300.

Authenticating administrators who use RSA SecurID to log on to the management server

If you want to authenticate administrators who use the Symantec Endpoint Protection Manager with RSA SecurID, you need to enable encrypted authentication by running the RSA installation wizard.

To authenticate administrators who use RSA SecurID to log on to the management server

- 1 Install an RSA ACE server, if necessary.
- 2 Register the computer on which you installed the management server as a valid host on the RSA ACE server.
- 3 Create the Node Secret file for the same host.
- 4 Ensure that the sdconf.rec file on the RSA ACE server is accessible on the network.
- 5 Assign a synchronized SecurID card or key fob to a management server account; activate the logon name on the RSA ACE server.
- 6 Ensure that the administrator has the RSA PIN or password available.

Symantec supports the following types of RSA logons:

- RSA SecurID token (not software RSA tokens)
- RSA SecurID card
- RSA keypad card (not RSA smart cards)

To log on to the management server with the RSA SecurID, the administrator needs a logon name, the token (hardware), and a pin number.

See [“Configuring the management server to authenticate administrators who use RSA SecurID to log on”](#) on page 298.

See [“Changing the authentication method for administrator accounts”](#) on page 297.

Best practices for testing whether a directory server authenticates an administrator account

You can test whether an Active Directory or LDAP server authenticates the user name and password for an administrator account that you create. The test also ensures that you added the user name and password correctly.

You use the same user name and password for an administrator account in Symantec Endpoint Protection Manager as you do in the directory server. When the administrator logs on to the management server, the directory server

Best practices for testing whether a directory server authenticates an administrator account

authenticates the administrator's user name and password. The management server uses the directory server configuration that you added to search for the account on the directory server.

The **Test Account** option checks whether or not the account name exists on the directory server.

You can also test whether an Active Directory or LDAP server authenticates an administrator account with no user name and password. An account with no user name or password is anonymous access. You should create an administrator account with anonymous access so that the administrators are never locked out if the password changes on the directory server.

Note: In Windows 2003 Active Directory server, anonymous authentication is disabled by default. Therefore, when you add a directory server without a user name to an administrator account and click **Test Account**, an **Account Authentication Failed** error message appears. To work around this issue, create two directory server entries, one for testing, and one for anonymous access. The administrator can still log on to the management server using a valid user name and password.

Table 12-4 Steps to test directory server authentication for an administrator account

Step	Task	Description
Step 1	Add multiple directory server connections	<p>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.</p> <p>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.</p> <p>Use the following information to set up the directory servers for this example:</p> <ul style="list-style-type: none"> ■ CN=John Smith ■ OU=test ■ DC=<sampledomain> ■ DC=local <p>The example uses the default Active Directory LDAP (389) but can also use Secure LDAP (636).</p>

Table 12-4 Steps to test directory server authentication for an administrator account (*continued*)

Step	Task	Description
Step 2	Add multiple administrator accounts	You add multiple system administrator accounts. The account for anonymous access does not have a user name or password. See “To add the administrator accounts using the directory server entries” on page 303.

To add the directory server connections to test Active Directory and LDAP server authentication

- 1 On the console, click **Admin > Servers**, select the default server, and click **Edit the server properties**.
- 2 On the **Directory Servers** tab, click **Add**.
- 3 On the **General** tab, add the following directory server configurations, and then click **OK**.

Directory server 1:

- **Name:** `<sampledomain> Active Directory`
- **Server Type:** **Active Directory**
- **Server IP Address or Name:** `server01.<sampledomain>.local`
- **User Name:** `<sampledomain>\administrator`
- **Password:** `<directory server password>`

Directory server 2:

- **Name:** `<sampledomain> LDAP with User Name`
- **Server Type:** **LDAP**
- **Server IP Address or Name:** `server01.<sampledomain>.local`
- **LDAP Port:** **389**
- **LDAP BaseDN:** `DC=<sampledomain>, DC=local`
- **User Name:** `<sampledomain>\administrator`
- **Password:** `<directory server password>`

Directory server 3 (for anonymous authentication):

- **Name:** `<sampledomain> LDAP without User Name`
- **Server Type:** **LDAP**

- **Server IP Address or Name:** `server01.<sampledomain>.local`
- **LDAP Port:** **389**
- **LDAP BaseDN:** `<empty>`
Leave this field empty when you use anonymous access.
- **User Name:** `<empty>`
- **Password:** `<empty>`
After you click **OK**, a warning appears. But the directory server is valid.
When you try to add a BaseDN without a user name and password, the warning appears.

To add the administrator accounts using the directory server entries

- 1 On the console, click **Admin > Administrators**, and on the **General** tab, add the administrator accounts in step 2.

See [“Adding an administrator account”](#) on page 295.

See [“Changing the authentication method for administrator accounts”](#) on page 297.

After you add each administrator account and click the **Test Account** option, you see a message. In some cases, the message appears to invalidate the account information. The administrator can still log on to Symantec Endpoint Protection Manager, however.

- 2 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 **Test 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 **Test 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 **Test Account**.
The system administrator john can log on into Symantec Endpoint Protection Manager with directory authentication.

Administrator account 4, for anonymous access:

- On the **General** tab, 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 **Test Account**.

The account authentication fails, but the system administrator `John Smith` can log on to Symantec Endpoint Protection Manager.

See [“Connecting Symantec Endpoint Protection Manager to a directory server”](#) on page 242.

Changing the password for an administrator account

For security purposes, you may need to change the password for your account or another administrator's account.

The following rules apply to changing passwords:

- System administrators can change the password for all administrators.
- Domain administrators can change the password for other domain administrators and limited administrators within the same domain.
- Limited administrators can change their own passwords only.

When you configure the management server in the Management Server Configuration Wizard, you select either the embedded database or a Microsoft SQL Server database. If you select the embedded database, the password you enter for the default administrator account `admin` also becomes the database password. If you change the default administrator's password, the database password does not change.

If you change the password to fix an administrator account lockout, the administrator must still wait for the lockout period to expire.

See [“Configuring an administrator's account to lock after too many logon attempts”](#) on page 84.

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 306.

See [“Displaying the Forgot your password? link so that administrators can reset lost passwords”](#) on page 307.

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 must have the ability to reset their own passwords.
 See [“Displaying the Forgot your password? link so that administrators can reset lost passwords”](#) on page 307.
- Enable the **Forgot your password?** link 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 82.
- The mail server must be configured so that the mail server sends the notification.
 See [“Establishing communication between the management server and email servers”](#) on page 628.

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.

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.

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 authentication method for administrator accounts”](#) on page 297.

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 perform disaster recovery to rebuild Symantec Endpoint Protection Manager. 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 [“Performing disaster recovery”](#) on page 737.

Resetting the password for 12.1.1 and earlier with the `ResetPass.bat` script

In versions 12.1 RU1 (12.1.1) and earlier, you can use the `ResetPass.bat` script, found in the `/Symantec Endpoint Protection Manager/Tools` installation folder. This script forcefully resets the default administrator account password to `admin` if it is not linked to an Active Directory account.

Symantec no longer supports the script. In versions 12.1 RU1 MP1 (12.1.1.1) and later, the script has not been tested and may cause damage to Symantec Endpoint Protection Manager or the database.

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 306.

See [“Displaying the Remember my user name and Remember my password check boxes on the logon screen”](#) on page 82.

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.

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 306.

See [“Configuring an administrator’s account to lock after too many logon attempts”](#) on page 84.

Managing domains

This chapter includes the following topics:

- [About domains](#)
- [Adding a domain](#)
- [Switching to the current domain](#)

About domains

When you install a management server, the Symantec Endpoint Protection Manager console includes one domain, which is called Default. A domain is a structural container in the console that you use to organize a hierarchy of groups, clients, computers, and policies. You set up additional domains to manage your network resources.

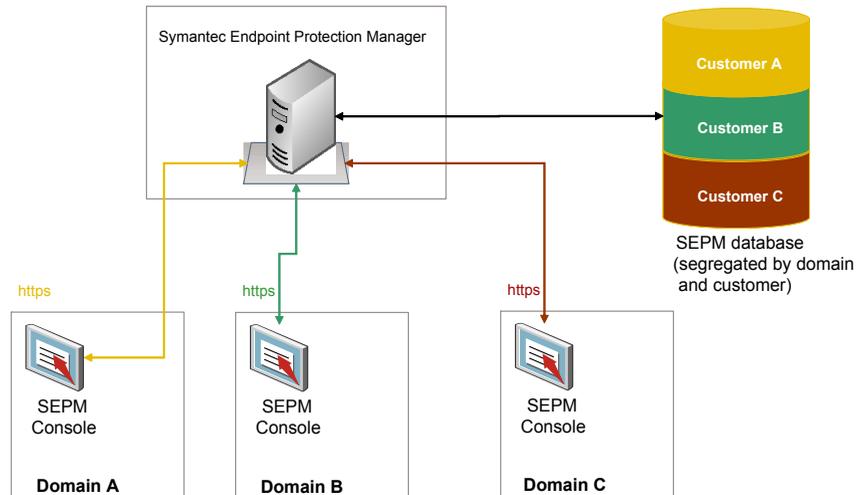
Note: The domains in Symantec Endpoint Protection Manager are not equivalent to Windows domains or other network domains.

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 13-1 Overview of Symantec Endpoint Protection Manager domains



When you add a domain, the domain is empty. You must set the domain to be the current domain. You then add 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 311.

See [“Managing administrator accounts”](#) on page 291.

See [“Switching to the current domain”](#) on page 311.

See [“Restoring client-server communication settings by using the SylinkDrop tool”](#) on page 752.

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 309.

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 309.

See [“Adding a domain”](#) on page 311.

Managing security policies

- [Chapter 14. Using policies to manage security](#)
- [Chapter 15. Managing firewall protection](#)
- [Chapter 16. Managing intrusion prevention](#)
- [Chapter 17. Managing Virus and Spyware Protection](#)
- [Chapter 18. Customizing scans](#)
- [Chapter 19. Managing SONAR](#)
- [Chapter 20. Managing Tamper Protection](#)
- [Chapter 21. Managing exceptions](#)
- [Chapter 22. Testing security policies](#)

Using policies to manage security

This chapter includes the following topics:

- [Manually updating policies on the client](#)
- [Performing the tasks that are common to all policies](#)
- [The types of security policies](#)
- [Adding a policy](#)
- [Editing a policy](#)
- [Copying and pasting a policy on the Policies page](#)
- [Copying and pasting a policy on the Clients page](#)
- [Assigning a policy to a group](#)
- [Replacing a policy](#)
- [Exporting and importing individual policies](#)
- [About shared and non-shared policies](#)
- [Converting a shared policy to a non-shared policy](#)
- [Withdrawing a policy from a group](#)
- [Locking and unlocking Virus and Spyware Protection policy settings](#)
- [Monitoring the applications and services that run on client computers](#)
- [Searching for information about the applications that the computers run](#)

Manually updating policies on the client

You can manually update the policies on the client computer if you do not think you have the latest policy on the client. If the client does not receive the update, there might be a communication problem.

Check the policy serial number to check whether your managed client computers can communicate with the management server.

You can only manually update the policy on the client computer.

See [“Using the policy serial number to check client-server communication”](#) on page 172.

To manually update policies on the client

- 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 **Update**.

See [“Performing the tasks that are common to all policies”](#) on page 315.

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 14-1](#) describes many of the policy tasks that you can perform.

Table 14-1 Tasks common to all policies

Task	Description
Add a policy	<p>If you do not want to use one of the default policies, you can add a new policy.</p> <p>You can add shared policies or non-shared policies.</p> <p>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.</p> <p>See “The types of security policies” on page 318.</p> <p>See “About shared and non-shared policies” on page 327.</p> <p>See “Adding a policy” on page 320.</p>
Lock and unlock policy settings	<p>You can lock and unlock some Virus and Spyware Protection policy settings. Computer users cannot change locked policy settings. A padlock icon appears next to a lockable policy setting.</p> <p>See “Locking and unlocking Virus and Spyware Protection policy settings” on page 330.</p>
Edit a policy	<p>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.</p> <p>See “Editing a policy” on page 321.</p>
Assign a policy	<p>To put a policy into use, you must assign it to one or more groups or locations.</p> <p>See “Assigning a policy to a group” on page 323.</p>
Test a policy	<p>Symantec recommends that you always test a new policy before you use it in a production environment.</p>
Update the policies on clients	<p>Based on the available bandwidth, you can configure a client to use push mode or pull mode as its policy update method.</p> <p>See “How the client computer and the management server communicate” on page 169.</p> <p>See “Configuring push mode or pull mode to update client policies and content” on page 170.</p>

Table 14-1 Tasks common to all policies (*continued*)

Task	Description
Replace a policy	<p>You can replace a shared policy with another shared policy. You can replace the shared policy in either all locations or for one location.</p> <p>See “Replacing a policy” on page 325.</p>
Copy and paste a policy	<p>Instead of adding a new policy, you may want to copy an existing policy to use as the basis for the new policy.</p> <p>You can copy and paste policies on either the Policies page or the Policies tab on the Clients page.</p> <p>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.</p> <p>See “Copying and pasting a policy on the Clients page” on page 322.</p> <p>See “Copying and pasting a policy on the Policies page” on page 322.</p>
Convert a shared policy to a non-shared policy	<p>You can copy the content of a shared policy and create a non-shared policy from that content.</p> <p>See “About shared and non-shared policies” on page 327.</p> <p>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.</p> <p>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.</p> <p>See “Converting a shared policy to a non-shared policy” on page 328.</p>
Export and import a policy	<p>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.</p> <p>See “Exporting and importing individual policies” on page 326.</p>

Table 14-1 Tasks common to all policies (*continued*)

Task	Description
Withdraw a policy	<p>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.</p> <p>You can withdraw any type of policy except a Virus and Spyware Protection policy and a LiveUpdate Settings policy.</p> <p>See “Withdrawing a policy from a group” on page 329.</p>
Delete a policy	<p>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</p>
Check that the client has the latest policy	<p>You can check whether the client has the latest policy. If not, you can manually update the policy on the client.</p> <p>See “How the client computer and the management server communicate” on page 169.</p> <p>See “Using the policy serial number to check client-server communication” on page 172.</p> <p>See “Manually updating policies on the client” on page 315.</p>

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 315.

Table 14-2 Security policy types

Policy type	Description
Virus and Spyware Protection policy	<p>The Virus and Spyware Protection policy provides the following protection:</p> <ul style="list-style-type: none"> ■ 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. <p>The Virus and Spyware Protection policy finds behavior anomalies through its SONAR technology.</p> <p>Note: Download Insight and SONAR technology are available only on Windows clients.</p> <p>See “Managing scans on client computers” on page 405.</p>
Firewall policy	<p>The Firewall policy provides the following protection:</p> <ul style="list-style-type: none"> ■ 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. <p>Note: Firewall policies can be applied only to Windows clients.</p> <p>See “Managing firewall protection” on page 336.</p>
Intrusion Prevention policy	<p>The Intrusion Prevention policy automatically detects and blocks network attacks and attacks on browsers.</p> <p>Note: Intrusion Prevention policies can be applied only to Windows clients.</p> <p>See “Managing intrusion prevention on client computers” on page 380.</p>
LiveUpdate policy	<p>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.</p> <p>See “Managing content updates” on page 181.</p>

Table 14-2 Security policy types (continued)

Policy type	Description
Application and Device Control	<p>The Application and Device Control policy protects a system's resources from applications and manages the peripheral devices that can attach to computers.</p> <p>See "Setting up application and device control" on page 526.</p> <p>Note: Application and Device Control policies can be applied only to Windows clients.</p>
Host Integrity	<p>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.</p> <p>See "Setting up Host Integrity" on page 572.</p>
Exceptions policy	<p>The Exceptions policy provides the ability to exclude applications and processes from detection by the virus and spyware scans and by SONAR.</p> <p>You can also exclude applications from application control.</p> <p>See "Managing exceptions in Symantec Endpoint Protection" on page 495.</p>

Adding a policy

Symantec Endpoint Protection Manager comes with a default policy for each type of protection. If you need to customize a policy, you add one and edit it. You can create multiple versions of each type of policy.

Symantec recommends that you test all new policies before you use them in a production environment.

To add a new policy

- 1 In the console, click **Policies**.
- 2 On the **Policies** page, select a policy type, and then click the link to add a new policy.
- 3 Modify the policy settings to increase or decrease protection.

- 4 Click **OK** to save the policy.
- 5 Optionally assign the new policy to a group.
You can assign a new policy to a group during or after policy creation. The new policy replaces the currently assigned policy of the same protection type.
See [“Assigning a policy to a group”](#) on page 323.
See [“Performing the tasks that are common to all policies”](#) on page 315.

Editing a policy

You can edit shared and non-shared policies on the **Policies** tab on the **Clients** page as well as on the **Policies** page.

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

See [“Performing the tasks that are common to all policies”](#) on page 315.

To edit a policy in the Policies page

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

To edit a policy in the Clients page

- 1 In the console, click **Clients**.
- 2 On the **Clients** page, under **Clients**, select the group for which you want to edit a policy.
- 3 On the **Policies** tab, uncheck **Inherit policies and settings from parent group "group name"**.
You must disable inheritance for this group. If you do not uncheck inheritance, you cannot edit a policy.
- 4 Under **Location-specific Policies and Settings**, scroll to find the name of the location whose policy you want to edit.
- 5 Locate the specific policy for the location that you want to edit.
- 6 To the right of the selected policy, click **Tasks**, and then click **Edit Policy**.

- 7 Do one of the following tasks:
 - To edit a non-shared policy, go to step 8.
 - To edit a shared policy, in the **Edit Policy** dialog box, click **Edit Shared** to edit the policy in all locations.
- 8 You can click a link for the type of policy that you want to edit.

Copying and pasting a policy on the Policies page

You can copy and paste a policy on the **Policies** page. For example, you may want to edit the policy settings slightly to apply to another group.

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 322.

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 315.

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

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 clients that run different platforms. If you put clients that run different platforms into the same group, be aware that 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 user interface in the **Assign policy** dialog box conveys the following additional information:

A folder icon indicates a group.



A round icon indicates a location.



- On a group icon, a check mark in a green circle indicates that this policy is assigned to all of the locations in the group.
- On a location icon, a check mark in a green circle indicates that this policy is assigned to this location.
- Text that is grayed out means that the group or location inherits its policy from its parent group.

See [“Performing the tasks that are common to all policies”](#) on page 315.

To assign a policy to a group

- 1 In the console, click **Policies**.
- 2 On the **Policies** page, select a policy, and then click **Assign the policy**.
- 3 In the **Assign policy** dialog box, select the groups, and then click **Assign**.
- 4 Click **OK** to confirm.

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 315.

To replace a shared policy for all locations

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

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

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

You must disable inheritance for this group. If you do not uncheck inheritance, you cannot replace a policy.
- 4 Under **Location-specific Policies and Settings**, scroll to find the location that contains the policy.

- 5 Next to the policy that you want to replace, click **Tasks**, and then click **Replace Policy**.
- 6 In the **Replace Policy** dialog box, in the **New policy** list box, select the replacement policy.
- 7 Click **OK**.

Exporting and importing individual policies

You can export and import policies rather than recreating the policies. All the settings that are associated with the policy are automatically exported.

You may need to export a policy for the following reasons:

- You update the management server from an older release to a newer release. You want to update the new management server with the policies that you previously customized.
- You want to export a policy for use at a different site.

You 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 315.

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 320.
 - Copy an existing policy to base the new policy on.
See [“Copying and pasting a policy on the Policies page”](#) on page 322.
See [“Copying and pasting a policy on the Clients page”](#) on page 322.
 - Import a policy that was previously exported from another site.
See [“Exporting and importing individual policies”](#) on page 326.
- See [“Performing the tasks that are common to all policies”](#) on page 315.
- See [“Converting a shared policy to a non-shared policy”](#) on page 328.

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 327.

See [“Copying and pasting a policy on the Policies page”](#) on page 322.

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 315.

Withdrawing a policy from a group

You may want to withdraw a policy from a group or a location under certain circumstances.

For example, a specific group may have experienced problems after you introduced a new policy. If you want the policy to remain in the database, you can withdraw the policy instead of deleting it. If you withdraw a policy, it is automatically withdrawn from the groups and locations that you assigned it to. The number of locations that a policy is used for appears on the **policy type Policies** pane on the **Policies** page.

Note: You must withdraw a policy or replace a policy from all groups and locations before you can delete it.

You can withdraw all policies in the **Policies** page from a location or group except for the following policies:

- **Virus and Spyware Protection**
- **LiveUpdate Settings**

You can only replace them with another **Virus and Spyware Protection policy** or **LiveUpdate policy**.

See [“Replacing a policy”](#) on page 325.

See [“Assigning a policy to a group”](#) on page 323.

To withdraw a shared policy in the Policies page

- 1 In the console, click **Policies**.
- 2 On the **Policies** page, under **Policies**, click the type of policy that you want to withdraw.
- 3 In the **policy type Policies** pane, click the specific policy that you want to withdraw.
- 4 On the **Policies** page, under **Tasks**, click **Withdraw the Policy**.
- 5 In the **Withdraw Policy** dialog box, check the groups and locations from which you want to withdraw the policy.
- 6 Click **Withdraw**.
- 7 When you are prompted to confirm the withdrawal of the policy from the groups and locations, click **Yes**.

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

- 1 In the console, click **Clients**.
- 2 On the **Clients** page, under **Clients**, select the group for which you want to withdraw a policy.
- 3 On the **Policies** tab, uncheck **Inherit policies and settings from parent group "group name"**.
You must disable inheritance for this group. If you do not uncheck inheritance, you cannot withdraw a policy.
- 4 Under **Location-specific Policies and Settings**, scroll to find the name of the location for which you want to withdraw a policy.
- 5 Locate the policy for the location that you want to withdraw.
- 6 Click **Tasks**, and then click **Withdraw Policy**.
- 7 In the **Withdraw Policy** dialog box, click **Yes**.

See [“Performing the tasks that are common to all policies”](#) on page 315.

Locking and unlocking Virus and Spyware Protection policy settings

You can lock and unlock some Virus and Spyware Protection policy settings. End users cannot change locked settings. A padlock icon appears next to a lockable setting.

See [“About access to the client interface on Windows clients”](#) on page 266.

See [“Performing the tasks that are common to all policies”](#) on page 315.

To lock or unlock a policy setting

- 1 In the console, open a Virus and Spyware Protection policy.
- 2 Select one of the pages, such as **Auto-Protect**.
- 3 Click a padlock icon to lock or unlock the corresponding setting.
- 4 Click **OK**.

You can also lock and unlock Tamper Protection settings, Submissions settings, and intrusion prevention settings.

See [“Changing Tamper Protection settings”](#) on page 494.

See [“Enabling or disabling client submissions to Symantec Security Response”](#) on page 442.

See [“Enabling or disabling network intrusion prevention or browser intrusion prevention”](#) on page 386.

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 14-3 Steps to monitor the applications

Steps	Description
Enable learned applications	<p>Configure the management server to collect information about the applications that the client computers run.</p> <p>See “Configuring the management server to collect information about the applications that the client computers run” on page 332.</p>
Search for applications	<p>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.</p> <p>See “Searching for information about the applications that the computers run” on page 333.</p> <p>You can save the results of an application search for review.</p>

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

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

You can enable learned applications for a group or a location. The clients then keep track of every application that runs and send that data to the management server.

Note: The Mac 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 630.

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 315.

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 356.

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 315.

Managing firewall protection

This chapter includes the following topics:

- [Managing firewall protection](#)
- [Creating a firewall policy](#)
- [Managing firewall rules](#)
- [Setting up firewall rules](#)

Managing firewall protection

The firewall allows the incoming network traffic and outgoing network traffic that you specify in firewall policy. The Symantec Endpoint Protection firewall policy contains rules and protection settings, most of which you can enable or disable and configure.

[Table 15-1](#) describes ways in which you can manage your firewall protection. All of these tasks are optional.

Table 15-1 Manage firewall protection

Task	Description
Read about firewall protection	Before you configure your firewall protection, you should familiarize yourself with the firewall. See “How a firewall works” on page 337. See “About the Symantec Endpoint Protection firewall” on page 338.

Table 15-1 Manage firewall protection (*continued*)

Task	Description
Create a firewall policy	<p>Symantec Endpoint Protection installs with a default firewall policy. You can modify the default policy or create new ones.</p> <p>You must create a policy first before you configure firewall rules and firewall protection settings for that policy.</p> <p>See “Creating a firewall policy” on page 339.</p> <p>See “Enabling and disabling a firewall policy” on page 342.</p>
Create and customize firewall rules	<p>Firewall rules are the policy components that control how the firewall protects client computers from malicious attacks.</p> <p>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.</p> <p>See “Managing firewall rules” on page 348.</p> <p>See “Setting up firewall rules” on page 367.</p>
Enable firewall protection settings	<p>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.</p> <p>See “Automatically allowing communications for essential network services” on page 343.</p> <p>See “Automatically blocking connections to an attacking computer” on page 345.</p> <p>See “Detecting potential attacks and spoofing attempts” on page 346.</p> <p>See “Preventing stealth detection” on page 347.</p> <p>See “Disabling the Windows firewall” on page 347.</p> <p>See “Configuring peer-to-peer authentication for Host Integrity enforcement” on page 582.</p>
Monitor firewall protection	<p>Regularly monitor the firewall protection status on your computers.</p> <p>See “Monitoring endpoint protection” on page 593.</p>

See [“Running commands on client computers from the console”](#) on page 261.

See [“Configuring firewall settings for mixed control”](#) on page 344.

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 enable or disable the firewall protection as needed.

You can install the client with default firewall settings. In most cases you do not have to change the settings. However, if you have a detailed understanding of networks, you can make many changes in the client firewall to fine-tune the client computer's protection.

See [“Managing firewall protection”](#) on page 336.

See [“How a firewall works”](#) on page 337.

See [“How the firewall uses stateful inspection”](#) on page 355.

See [“The types of security policies”](#) on page 318.

Creating a firewall policy

The Symantec Endpoint Protection includes a default Firewall policy with default firewall rules and default firewall settings for the office environment. The office environment is normally under the protection of corporate firewalls, boundary packet filters, or antivirus servers. Therefore, it is normally more secure than most home environments, where limited boundary protection is available.

When you install the console for the first time, it adds a default Firewall policy to each group automatically.

Every time you add a new location, the console copies a Firewall policy to the default location automatically. If the default protection is not appropriate, you can customize the Firewall policy for each location, such as for a home site or customer site. If you do not want the default Firewall policy, you can edit it or replace it with another shared policy.

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

- The default firewall protection blocks inbound and outbound IPv6 traffic with all remote systems.

Note: IPv6 is a network layer protocol that is used on the Internet. If you install the client on the computers that run Microsoft Vista, the **Rules** list includes several default rules that block the Ethernet protocol type of IPv6. If you remove the default rules, you must create a rule that blocks IPv6.

- The default firewall protection restricts the inbound connections for a few protocols that are often used in attacks (for example, Windows file sharing). Internal network connections are allowed and external networks are blocked.

[Table 15-2](#) describes the tasks that you can perform to configure a new firewall policy. You must add a firewall policy first, but thereafter, the remaining tasks are optional and you can complete them in any order.

Table 15-2 How to create a firewall policy

Task	Description
Add a firewall policy	<p>When you create a new policy, you give it a name and a description. You also specify the groups to which the policy is applied.</p> <p>A firewall policy is automatically enabled when you create it. But you can disable it if you need to.</p> <p>See “Enabling and disabling a firewall policy” on page 342.</p>
Create firewall rules	<p>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.</p> <p>When you create a new Firewall policy, Symantec Endpoint Protection provides default firewall rules.</p> <p>The default firewall rules are enabled by default.</p> <p>See “Setting up firewall rules” on page 367.</p>

Table 15-2 How to create a firewall policy (*continued*)

Task	Description
<p>Enable and customize notifications to users that access to an application is blocked</p>	<p>You can send users a notification that an application that they want to access is blocked.</p> <p>These settings are disabled by default.</p> <p>See “Notifying the users that access to an application is blocked” on page 360.</p>
<p>Enable automatic firewall rules</p>	<p>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.</p> <p>Only the traffic protocols are enabled by default.</p> <p>See “Automatically allowing communications for essential network services” on page 343.</p> <p>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.</p> <p>This option is disabled by default.</p> <p>See “Automatically blocking connections to an attacking computer” on page 345.</p>
<p>Configure protection and stealth settings</p>	<p>You can enable settings to detect and log potential attacks on the client and block spoofing attempts.</p> <p>See “Detecting potential attacks and spoofing attempts” on page 346.</p> <p>You can enable the settings that prevent outside attacks from detecting information about your clients.</p> <p>See “Preventing stealth detection” on page 347.</p> <p>All of the protection options and stealth options are disabled by default.</p>

Table 15-2 How to create a firewall policy (*continued*)

Task	Description
Integrate the Symantec Endpoint Protection firewall with the Windows firewall	<p>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.</p> <p>The default setting is to disable the Windows firewall once only and to disable the Windows firewall disabled message.</p> <p>See “Disabling the Windows firewall” on page 347.</p>
Configure peer-to-peer authentication	<p>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.</p> <p>This option is disabled by default.</p> <p>See “Configuring peer-to-peer authentication for Host Integrity enforcement” on page 582.</p>

See [“Managing firewall protection”](#) on page 336.

See [“Best practices for Firewall policy settings”](#) on page 287.

See [“Editing a policy”](#) on page 321.

Enabling and disabling a firewall policy

Firewall policies are automatically enabled when you create them. You can disable a firewall policy as needed, and then enable it again. You must enable a firewall policy for it to be active.

You might want to disable the firewall for any of the following reasons:

- You install an application that might cause the firewall to block it.
- A firewall rule or firewall setting blocks an application due to an administrator's mistake.
- The firewall causes network connectivity-related issues.
- The firewall might slow down the client computer.

You should enable at least the default firewall protection to keep your computers protected during remote client installation.

See [“About enabling and disabling protection when you need to troubleshoot problems”](#) on page 256.

To enable or disable a firewall policy

- 1 In the console, click **Policies**.
- 2 On the **Policies** page, select the Firewall policy, and then right-click **Edit**.
- 3 In the policy, on the **Overview** page, check **Enable this policy** to enable the policy; uncheck it to disable it.
- 4 Click **OK**.

See [“Creating a firewall policy”](#) on page 339.

See [“Managing firewall protection”](#) on page 336.

Automatically allowing communications for essential network services

You can enable the options that automatically permit communication between certain network services so you do not have to define the rules that explicitly allow those services. You can also enable traffic settings to detect and block the traffic that communicates through NetBIOS and token rings.

You can allow outbound requests and inbound replies for the network connections that are configured to use DHCP, DNS, and WINS traffic.

The filters allow DHCP, DNS, or WINS clients to receive an IP address from a server. It also protects the clients against attacks from the network with the following conditions:

If the client sends a request to the server	The client waits for five seconds to allow an inbound response.
---	---

If the client does not send a request to the server	Each filter does not allow the packet.
---	--

When you enable these options, Symantec Endpoint Protection permits the packet if a request was made; it does not block packets. You must create a firewall rule to block packets.

Note: To configure these settings in mixed control, you must also enable these settings in the **Client User Interface Mixed Control Settings** dialog box.

To automatically allow communications for essential network services

- 1 In the console, open a Firewall policy.
 - 2 On the **Firewall Policy** page, click **Built-in Rules**.
 - 3 Check the options that you want to enable.
 - 4 Click **OK**.
 - 5 If you are prompted, assign the policy to a location.
- See [“Creating a firewall policy”](#) on page 339.
- See [“Editing a policy”](#) on page 321.
- See [“Locking and unlocking settings by changing the user control level”](#) on page 267.

Configuring firewall settings for mixed control

You can configure the client so that users have no control, full control, or limited control over which firewall settings they can configure.

Use the following guidelines when you configure the client:

Server control	The user cannot create any firewall rules or enable firewall settings.
Client control	The user can create firewall rules and enable all firewall settings.
Mixed control	The user can create firewall rules. You decide which firewall settings the user can enable.

To configure firewall settings for mixed control

- 1 In the console, click **Clients**.
- 2 Under **Clients**, select the group with the user control level that you want to modify.
- 3 On the **Policies** tab, under **Location-specific Policies and Settings**, under a location, expand **Location-specific Settings**.
- 4 To the right of **Client User Interface Control Settings**, click **Tasks > Edit Settings**.
- 5 In the **Control Mode Settings** dialog box, click **Mixed control**, and then click **Customize**.
- 6 On the **Client/Server Control Settings** tab, under the **Firewall Policy** category, do one of the following tasks:

- To make a client setting available for the users to configure, click **Client**.
 - To configure a client setting, click **Server**.
- 7 Click **OK**.
 - 8 Click **OK**.
 - 9 For each firewall setting that you set to **Server**, enable or disable the setting in the Firewall policy.
- See [“Managing firewall protection”](#) on page 336.
- See [“Automatically allowing communications for essential network services”](#) on page 343.
- See [“Detecting potential attacks and spoofing attempts”](#) on page 346.
- See [“Running commands on client computers from the console”](#) on page 261.

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 **Protection and Stealth**.
- 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 339.

See [“Configuring firewall settings for mixed control”](#) on page 344.

See [“Editing a policy”](#) on page 321.

Detecting potential attacks and spoofing attempts

You can enable the various settings that enable Symantec Endpoint Protection to detect and log potential attacks on the client and block spoofing attempts. All of these options are disabled by default.

The settings that you can enable are as follows:

Enable port scan detection When this setting is enabled, Symantec Endpoint Protection monitors all incoming packets that any security rule blocks. If a rule blocks several different packets on different ports in a short period of time, Symantec Endpoint Protection creates a Security log entry.

Port scan detection does not block any packets. You must create a security policy to block traffic when a port scan occurs.

Enable denial of service detection Denial of service detection is a type of intrusion detection. When enabled, the client blocks traffic if it detects a pattern from known signatures, regardless of the port number or type of Internet protocol.

Enable anti-MAC spoofing When enabled, Symantec Endpoint Protection allows incoming and outgoing address resolution protocol (ARP) traffic if an ARP request was made to that specific host. All other unexpected ARP traffic is blocked and an entry is generated to the Security log.

Note: To configure these settings in mixed control, you must also enable these settings in the **Client User Interface Mixed Control Settings** dialog box.

To detect potential attacks and spoofing attempts

- 1 In the console, open a Firewall policy.
- 2 In the **Firewall Policy** page, click **Protection and Stealth**.
- 3 Under **Protection Settings**, check any of the options that you want to enable.
- 4 Click **OK**.
- 5 If you are prompted, assign the policy to a location.

See [“Creating a firewall policy”](#) on page 339.

See [“Locking and unlocking settings by changing the user control level”](#) on page 267.

See [“Editing a policy”](#) on page 321.

Preventing stealth detection

You can enable the settings that prevent outside attacks from detecting information about your clients. These settings are disabled by default.

Note: To configure these settings in mixed control, you must also enable these settings in the **Client User Interface Mixed Control Settings** dialog box.

To prevent stealth detection

- 1 In the console, open a Firewall policy.
- 2 In the **Firewall Policy** page, click **Protection and Stealth**.
- 3 Under **Stealth Settings**, check any of the options that you want to enable as follows:

Enable stealth mode Web browsing Prevents the Web sites from knowing which operating system and browser your clients use.

Enable TCP resequencing Randomizes the TCP sequencing number to evade operating system fingerprinting and some kinds of IP spoofing.

Enable OS fingerprint masquerading Prevents the programs from detecting the operating system of the computer on which the firewall runs.

- 4 Click **OK**.
- 5 If you are prompted, assign the policy to a location.

See [“Creating a firewall policy”](#) on page 339.

See [“Locking and unlocking settings by changing the user control level”](#) on page 267.

See [“Editing a policy”](#) on page 321.

Disabling the Windows firewall

You can specify the conditions in which Symantec Endpoint Protection disables the Windows firewall. When Symantec Endpoint Protection is uninstalled, Symantec

Endpoint Protection restores the Windows firewall setting to the state it was in before Symantec Endpoint Protection was installed.

Note: Symantec Endpoint Protection does not modify any existing Windows firewall policy rules or exclusions.

Typically, a Windows user receives a notification when their computer restarts if the Windows firewall is disabled. Symantec Endpoint Protection disables this notification by default so that it does not alarm your users when the Windows firewall is disabled. But you can enable the notification, if desired.

To disable the Windows firewall

- 1 In the console, click **Policies**.
- 2 Under **Policies**, click **Firewall**.
- 3 Do one of the following tasks:
 - Create a new firewall policy.
 - In the **Firewall Policies** list, double-click on the firewall policy that you want to modify.
- 4 Under **Firewall Policy**, click **Windows Integration**.
- 5 In the **Disable Windows Firewall** drop-down list, specify when you want the Windows firewall disabled.

The default setting is **Disable Once Only**.

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 the Windows firewall is disabled.

- 7 Click **OK**.

See [“Creating a firewall policy”](#) on page 339.

See [“The types of security policies”](#) on page 318.

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 15-3](#) describes what you need to know to manage firewall rules.

Table 15-3 Managing firewall rules

Subject	Description
<p>Learn how firewall rules work and what makes up a firewall rule</p>	<p>Before you modify the firewall rules, you should understand the following information about how firewall rules work:</p> <ul style="list-style-type: none"> ■ 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 350. ■ 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 351. ■ The implications of inheriting rules from a parent group and how inherited rules are processed See “About inherited firewall rules” on page 352. ■ 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 355. ■ 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 356. See “About firewall rule host triggers” on page 360. See “About firewall rule network services triggers” on page 364. See “About firewall rule network adapter triggers” on page 365.

Table 15-3 Managing firewall rules (*continued*)

Subject	Description
Add a new firewall rule	<p>You can perform the following tasks to manage firewall rules:</p> <ul style="list-style-type: none"> ■ 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 368. ■ 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 369. ■ 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.
Enable or disable a firewall rule	<p>Firewall rules are automatically enabled. However, you may need to temporarily disable a firewall rule to test the rule. The firewall does not inspect disabled rules.</p>
Customize a firewall rule	<p>After you create a new rule, or if you want to customize a default rule, you can modify any of the firewall rule criteria.</p> <p>See “Customizing firewall rules” on page 370.</p>

See [“Managing firewall protection”](#) on page 336.

About firewall server rules and client rules

Rules are categorized as either server rules or client rules. Server rules are the rules that you create in Symantec Endpoint Protection Manager and that are downloaded to the Symantec Endpoint Protection client. Client rules are the rules that the user creates on the client.

[Table 15-4](#) describes the relationship between the client's user control level and the user's interaction with the firewall rules.

Table 15-4 User control level and rule status

User control level	User interaction
Server control	<p>The client receives server rules but the user cannot view them. The user cannot create client rules.</p>
Mixed control	<p>The client receives server rules. The user can create client rules, which are merged with server rules and client security settings.</p>

Table 15-4 User control level and rule status (*continued*)

User control level	User interaction
Client control	The client does not receive server rules. The user can create client rules. You cannot view client rules.

[Table 15-5](#) lists the order that the firewall processes server rules, client rules, and client settings.

Table 15-5 Server rules and client rules processing priority

Priority	Rule type or setting
First	Server rules with high priority levels (rules above the blue line in the Rules list)
Second	Client rules
Third	Server rules with lower priority levels (rules under the blue line in the Rules list) On the client, server rules under the blue line are processed after client rules.
Fourth	Client security settings
Fifth	Client application-specific settings

On the client, users can modify a client rule or security setting, but users cannot modify a server rule.

Warning: If the client is in mixed control, users can create a client rule that allows all traffic. This rule overrides all server rules under the blue line.

See [“Managing firewall rules”](#) on page 348.

See [“Changing the order of firewall rules”](#) on page 354.

See [“Locking and unlocking settings by changing the user control level”](#) on page 267.

About the firewall rule, firewall setting, and intrusion prevention processing order

Firewall rules are ordered sequentially, from highest to lowest priority in the rules list. If the first rule does not specify how to handle a packet, the firewall inspects the second rule. This process continues until the firewall finds a match. After the

firewall finds a match, the firewall takes the action that the rule specifies. Subsequent lower priority rules are not inspected. For example, if a rule that blocks all traffic is listed first, followed by a rule that allows all traffic, the client blocks all traffic.

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

The Rules list contains a blue dividing line. The dividing line sets the priority of rules in the following situations:

- When a subgroup inherits rules from a parent group.
- When the client is set to mixed control. The firewall processes both server rules and client rules.

[Table 15-6](#) shows the order in which the firewall processes the rules, firewall settings, and intrusion prevention settings.

Table 15-6 Processing order

Priority	Setting
First	Custom IPS signatures
Second	Intrusion Prevention settings, traffic settings, and stealth settings
Third	Built-in rules
Fourth	Firewall rules
Fifth	Port scan checks
Sixth	IPS signatures that are downloaded through LiveUpdate

See [“Changing the order of firewall rules”](#) on page 354.

See [“Managing firewall rules”](#) on page 348.

See [“How a firewall works”](#) on page 337.

See [“How intrusion prevention works”](#) on page 383.

About inherited firewall rules

A subgroup's policy can inherit only the firewall rules that are enabled in the parent group. When you have inherited the rules, you can disable them, but you cannot modify them. As the new rules are added to the parent group's policy, the new rules are automatically added to the inheriting policy.

When the inherited rules appear in the **Rules** list, they are shaded in purple. Above the blue line, the inherited rules are added above the rules that you created. Below the blue line, the inherited rules are added below the rules that you created.

A Firewall policy also inherits default rules, so the subgroup's Firewall policy may have two sets of default rules. You may want to delete one set of default rules.

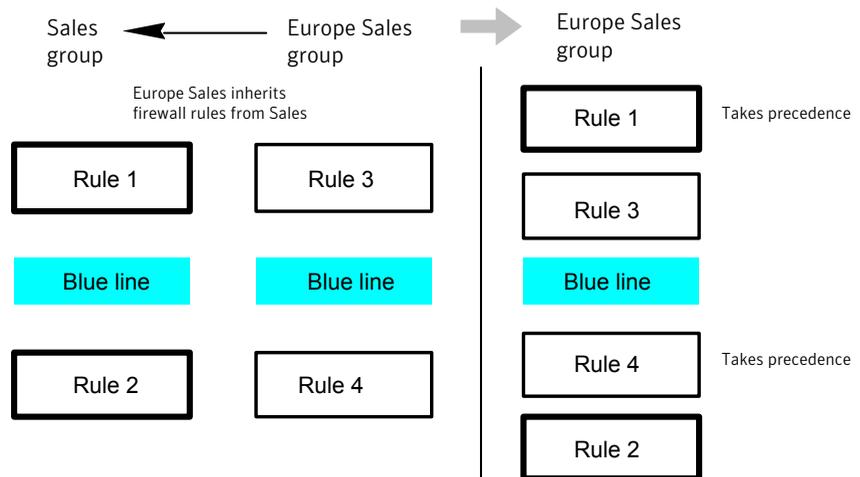
If you want to remove the inherited rules, you remove the inheritance rather than delete them. You have to remove all the inherited rules rather than the selected rules.

The firewall processes inherited firewall rules in the **Rules** list as follows:

- Above the blue dividing line The rules that the policy inherits take precedence over the rules that you create.
- Below the blue dividing line The rules that you create take precedence over the rules that the policy inherits.

[Figure 15-1](#) 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 15-1 An example of how firewall rules inherit from each other



See [“Managing firewall rules”](#) on page 348.

See [“Adding inherited firewall rules from a parent group”](#) on page 354.

Adding inherited firewall rules from a parent group

You can add firewall rules to a firewall policy by inheriting rules from a parent group. To inherit the rules from a parent group, the subgroup's policy must be a non-shared policy.

Note: If the group inherits all of its policies from a parent group, this option is unavailable.

To add inherited firewall rules from a parent group

- 1 In the console, open a Firewall policy.
- 2 On the **Firewall Policy** page, click **Rules**.
- 3 On the **Rules** tab, check **Inherit Firewall Rules from Parent Group**.
To remove the inherited rules, uncheck **Inherit Firewall Rules from Parent Group**.
- 4 Click **OK**.

See [“Editing a policy”](#) on page 321.

See [“About inherited firewall rules”](#) on page 352.

See [“Managing firewall rules”](#) on page 348.

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 351.

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 321.

See [“Managing firewall rules”](#) on page 348.

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 337.

See [“Managing firewall rules”](#) on page 348.

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 356.

See [“Notifying the users that access to an application is blocked”](#) on page 360.

See [“Managing firewall rules”](#) on page 348.

See [“Blocking networked applications that might be under attack”](#) on page 358.

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 357.
- 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 357.

Note: Network Application Monitoring must be enabled to define a firewall rule by all fields except for the path and file name. If Network Application Monitoring is disabled, rule processing ignores the content in those fields.

To define information about applications manually

- 1 In the console, open a Firewall policy.
- 2 On the **Firewall Policies** page, click **Rules**.
- 3 On the **Rules** tab, in the **Rules** list, right-click the **Application** field, and then click **Edit**.
- 4 In the **Application List** dialog box, click **Add**.
- 5 In the **Add Application** dialog box, enter one or more of the following fields:
 - Path and file name
 - Description
 - Size, in bytes
 - Date that the application was last changed
 - File fingerprint
- 6 Click **OK**.
- 7 Click **OK**.

To search for applications from the learned applications list

- 1 On the **Firewall Policies** page, click **Rules**.
- 2 On the **Rules** tab, select a rule, right-click the **Application** field, and then click **Edit**.
- 3 In the **Application List** dialog box, click **Add From**.
- 4 In the **Search for Applications** dialog box, search for an application.
- 5 Under the **Query Results** table, to add the application to the **Applications** list, select the application, click **Add**, and then click **OK**.
- 6 Click **Close**.
- 7 Click **OK**.

See [“Managing firewall rules”](#) on page 348.

See [“Editing a policy”](#) on page 321.

See [“About firewall rule application triggers”](#) on page 356.

Blocking networked applications that might be under attack

Network application monitoring tracks an application's behavior in the security log. If an application's content is modified too frequently, it is likely that a Trojan horse attacked the application and the client computer is not safe. If an application's content is modified on an infrequent basis, it is likely that a patch was installed and the client computer is safe. You can use this information to create a firewall rule that allows or blocks an application.

You can configure the client to detect and monitor any application that runs on the client computer and that is networked. Network applications send and receive traffic. The client detects whether an application's content changes.

If you suspect that a Trojan horse has attacked an application, you can use network application monitoring to configure the client to block the application. You can also configure the client to ask users whether to allow or block the application.

An application's content changes for the following reasons:

- A Trojan horse attacked the application.
- The application was updated with a new version or an update.

You can add applications to a list so that the client does not monitor them. You may want to exclude the applications that you think are safe from a Trojan horse attack, but that have frequent and automatic patch updates.

You may want to disable network application monitoring if you are confident that the client computers receive adequate protection from antivirus and antispyware protection. You may also want to minimize the number of notifications that ask users to allow or block a network application.

To block networked applications that might be under attack

- 1 In the console, click **Clients**.
- 2 Under **Clients**, select a group, and then click **Policies**.
- 3 On the **Policies** tab, under **Location-independent Policies and Settings**, click **Network Application Monitoring**.
- 4 In the **Network Application Monitoring for *group name*** dialog box, click **Enable Network Application Monitoring**.

5 In the **When an application change is detected** drop-down list, select the action that the firewall takes on the application that runs on the client as follows:

Ask	Asks the user to allow or block the application.
Block the traffic	Blocks the application from running.
Allow and Log	Allows the application to run and records the information in the security log. The firewall takes this action on the applications that have been modified only.

6 If you selected **Ask**, click **Additional Text**.

7 In the **Additional Text** dialog box, type the text that you want to appear under the standard message, and then click **OK**.

8 To exclude an application from being monitored, under **Unmonitored Application List**, do one of the following tasks:

To define an application manually	Click Add , fill out one or more fields, and then click OK .
To define an application from a learned applications list	Click Add From . The learned applications list monitors both networked and non-networked applications. You must select networked applications only from the learned applications list. After you have added applications to the Unmonitored Applications List , you can enable, disable, edit, or delete them.

9 Check the box beside the application to enable it; uncheck it to disable it.

10 Click **OK**.

See [“Managing firewall rules”](#) on page 348.

See [“Notifying the users that access to an application is blocked”](#) on page 360.

See [“About firewall rule application triggers”](#) on page 356.

See [“Searching for information about the applications that the computers run”](#) on page 333.

See [“Configuring the management server to collect information about the applications that the client computers run”](#) on page 332.

Notifying the users that access to an application is blocked

You can send users a notification that an application that they want to access is blocked. This notification appears on the users' computers.

Note: Enabling too many notifications can not only overwhelm your users, but can also alarm them. Use caution when enabling notifications.

To notify the users that access to an application is blocked

- 1 In the console, open a Firewall policy.
- 2 On the **Firewall Policies** page, click **Rules**.
- 3 On the **Notifications** tab, check the following options that you want to apply:

Display notification on the computer when the client blocks an application A notification appears when the client blocks an application.

Add additional text to notification Click **Set Additional Text** and customize the notification.

Customizing the notification text is optional.

- 4 Click **OK**.

See [“Managing firewall protection”](#) on page 336.

See [“Enabling and disabling a firewall policy”](#) on page 342.

See [“Managing firewall rules”](#) on page 348.

See [“About firewall rule application triggers”](#) on page 356.

See [“Blocking networked applications that might be under attack”](#) on page 358.

About firewall rule host triggers

You specify the host on both sides of the described network connection when you define host triggers.

Traditionally, the way to express the relationship between hosts is referred to as being either the source or destination of a network connection.

You can define the host relationship in either one of the following ways:

Source and destination The source host and destination host is dependent on the direction of traffic. In one case the local client computer might be the source, whereas in another case the remote computer might be the source.

The source and the destination relationship are more commonly used in network-based firewalls.

Local and remote The local host is always the local client computer, and the remote host is always a remote computer that is positioned elsewhere on the network. This expression of the host relationship is independent of the direction of traffic.

The local and the remote relationship is more commonly used in host-based firewalls, and is a simpler way to look at traffic.

You can define multiple source hosts and multiple destination hosts.

Figure 15-2 illustrates the source relationship and destination relationship with respect to the direction of traffic.

Figure 15-2 The relationship between source and destination hosts

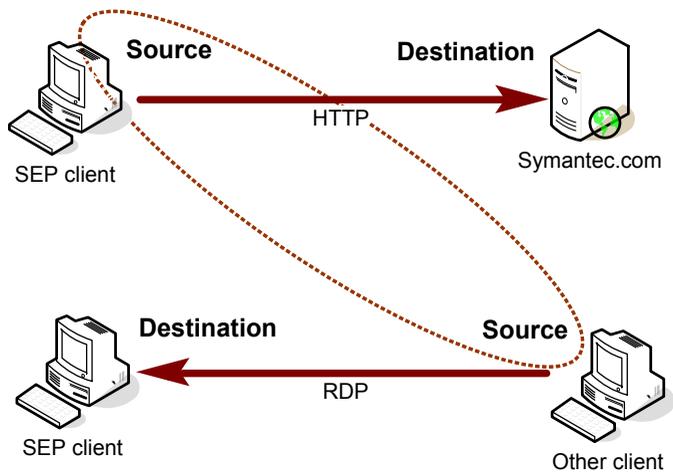
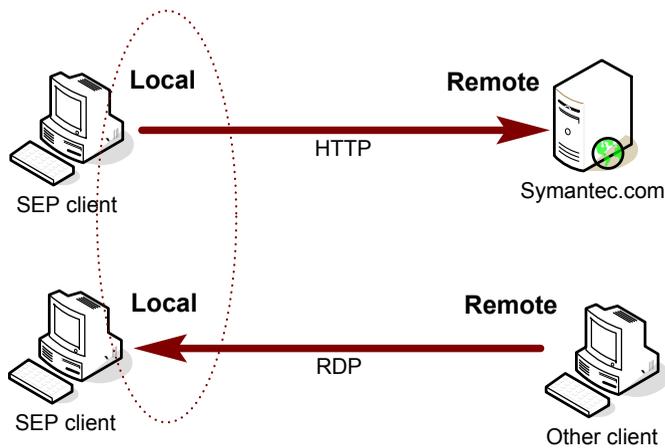


Figure 15-3 illustrates the local host and remote host relationship with respect to the direction of traffic.

Figure 15-3 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 362.

See [“Blocking traffic to or from a specific server”](#) on page 373.

See [“Managing firewall rules”](#) on page 348.

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 360.

Defining DNS queries based on location

You can define how frequently you want a specific location to perform a DNS query. This feature lets you configure one location to query the DNS server more often than other locations.

For example, assume that you have a policy to block all traffic outside of your corporate network except VPN traffic. And assume that your users travel and must access your network through a VPN from a hotel network. You can create a policy for a VPN connection that uses DNS resolution. Symantec Endpoint Protection continues to send the DNS query every 5 seconds until it switches to this location. This way, your users can more quickly access your network.

Caution: Use caution when you configure this setting to a very low value. You run the possibility of bringing down your DNS server if all of your systems access the server every 5 seconds, for example.

To define DNS queries based on location

- 1 In the console, click **Clients**.
- 2 Under **Clients**, select the group for which the feature applies.

- 3 Under **Tasks**, click **Manage Locations**.
 - 4 Ensure **DNS Query Loop in** is checked.
 - 5 Click the time setting and increments and modify as desired.
You can set the value in seconds, minutes, or hours.
The default value is 30 minutes.
 - 6 Click **OK**.
- See [“Managing firewall rules”](#) on page 348.
- See [“About firewall rule host triggers”](#) on page 360.

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 364.

See [“Permitting clients to browse for files and printers in the network”](#) on page 375.

See [“Managing firewall rules”](#) on page 348.

Adding network services to the default network services list

Network services let networked computers send and receive messages, share files, and print. You can create a firewall rule that allows or blocks network services.

The network services list eliminates the need to retype protocols and ports for the firewall rules that you create to block or allow network services. When you create a firewall rule, you can select a network service from a default list of commonly used network services. You can also add network services to the default list. However, you need to be familiar with the type of protocol and the ports that it uses.

Note: IPv4 and IPv6 are the two network layer protocols that are used on the Internet. The firewall blocks the attacks that travel through IPv4, but not through IPv6. If you install the client on the computers that run 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 348.

See [“About firewall rule network services triggers”](#) on page 364.

See [“Controlling whether networked computers can share messages, files, and printing”](#) on page 375.

See [“Permitting clients to browse for files and printers in the network”](#) on page 375.

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 348.

See [“Adding a custom network adapter to the network adapter list”](#) on page 366.

See [“Controlling the traffic that passes through a network adapter”](#) on page 378.

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 348.

See [“About firewall rule network adapter triggers”](#) on page 365.

See [“Controlling the traffic that passes through a network adapter”](#) on page 378.

Setting up firewall rules

[Table 15-7](#) describes how to set up new firewall rules.

Table 15-7 How to setup firewall rules

Step	Task	Description
Step 1	Add a new firewall rule	<p>You can add new firewall rules through the console using several methods. One method lets you add a blank rule that has default settings. The other method offers a wizard that guides you through creating a new rule.</p> <p>See “Adding a new firewall rule” on page 368.</p> <p>Another way that you can add a firewall rule is to export existing firewall rules from another Firewall policy. You can then import the firewall rules and settings so that you do not have to re-create them.</p> <p>See “Importing and exporting firewall rules” on page 369.</p> <p>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.</p>
Step 2	(Optional) Customize the firewall rule criteria	<p>After you create a new rule, or if you want to customize a default rule, you can modify any of the firewall rule criteria.</p> <p>See “Customizing firewall rules” on page 370.</p>

See [“Managing firewall rules”](#) on page 348.

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 368. |
| Add Firewall Rule wizard | If you add rules with the Add Firewall Rule wizard, ensure that you configure the rule. The wizard does not configure new rules with multiple criteria.

See "To add a new firewall rule using a wizard" on page 368. |

You should specify both the inbound and the outbound traffic in the rule whenever possible. You do not need to create inbound rules for traffic such as HTTP. The Symantec Endpoint Protection client uses stateful inspection for TCP traffic. Therefore, it does not need a rule to filter the return traffic that the clients initiate.

When you create a new firewall rule, it is automatically enabled. You can disable a firewall rule if you need to allow specific access to a computer or application. The rule is disabled for all inherited policies.

The rule is also disabled for the all locations if it is a shared policy and only one location if it is a location-specific policy.

Note: Rules must be enabled for the firewall to process them.

To add a new blank firewall rule

- 1 In the console, open a Firewall policy.
- 2 On the **Firewall Policy** page, click **Rules**.
- 3 On the **Rules** tab, under the **Rules** list, click **Add Blank Rule**.
- 4 Optionally, you can customize the firewall rule criteria as needed.
- 5 If you are done with the configuration of the rule, click **OK**.

To add a new firewall rule using a wizard

- 1 In the console, open a Firewall policy.
- 2 On the **Firewall Policy** page, click **Rules**.
- 3 On the **Rules** tab, under the **Rules** list, click **Add Rule**.
- 4 In the **Add Firewall Rule Wizard**, click **Next**.
- 5 In the **Select Rule Type** panel, select one of the types of rules.
- 6 Click **Next**.

- 7 Enter data on each panel to create the type of rule you selected.
 - 8 For applications and hosts, click **Add More** to add additional applications and services.
 - 9 When you are done, click **Finish**.
 - 10 Optionally, you can customize the firewall rule criteria as needed.
 - 11 If you are done with the configuration of the rule, click **OK**.
- See [“Customizing firewall rules”](#) on page 370.
- See [“Setting up firewall rules”](#) on page 367.
- See [“Editing a policy”](#) on page 321.
- See [“How the firewall uses stateful inspection”](#) on page 355.

Importing and exporting firewall rules

You can export and import firewall rules and settings from another Firewall policy so that you do not have to re-create them. For example, you can import a partial rule set from one policy into another. To import rules, you first have to export the rules to a .dat file and have access to the file.

The rules are added in the same order that they are listed in the parent policy with respect to the blue line. You can then change their processing order.

To export firewall rules

- 1 In the console, open a Firewall policy.
- 2 On the **Firewall Policy** page, click **Rules**.
- 3 In the **Rules** list, select the rules you want to export, right-click, and then click **Export**.
- 4 In the **Export Policy** dialog box, locate a directory to save the .dat file, type a file name, and then click **Export**.

To import firewall rules

- 1 In the console, open a Firewall policy.
- 2 On the **Firewall Policy** page, click **Rules**.
- 3 Right-click the Rules list, and then click **Import**.
- 4 In the **Import Policy** dialog box, locate the .dat file that contains the firewall rules to import, and then click **Import**.
- 5 In the **Input** dialog box, type a new name for the policy, and then click **OK**.
- 6 Click **OK**.

See [“Setting up firewall rules”](#) on page 367.

See [“Customizing firewall rules”](#) on page 370.

See [“About the firewall rule, firewall setting, and intrusion prevention processing order”](#) on page 351.

See [“Editing a policy”](#) on page 321.

Customizing firewall rules

When you create a new Firewall policy, the policy includes several default rules. You can modify one or multiple rule components as needed.

The components of a firewall rule are as follows:

Actions The action parameters specify what actions the firewall takes when it successfully matches a rule. If the rule matches and is selected in response to a received packet, the firewall performs all actions. The firewall either allows or blocks the packet and logs or does not log the packet. If the firewall allows traffic, it lets the traffic that the rule specifies access the network. If the firewall blocks traffic, it blocks the traffic that the rule specifies so that it does not access the network.

The actions are as follows:

- **Allow**
The firewall allows the network connection.
- **Block**
The firewall blocks the network connection.

Triggers	<p>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.</p> <p>The triggers are as follows:</p> <ul style="list-style-type: none"> ■ 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 356. ■ 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 360. ■ 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 364. ■ 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 365.
Conditions	<p>Rule conditions consist of the rule schedule and screen saver state.</p> <p>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.</p>

Notifications The Log settings let you specify whether the server creates a log entry or sends an email message when a traffic event matches the criteria that are set for this rule.

The Severity setting lets you specify the severity level of the rule violation.

Customizing firewall rules

- 1 In the console, open a Firewall policy.
- 2 On the **Firewall Policy** page, click **Rules**.
- 3 On the **Rules** tab, in the **Rules** list, in the **Enabled** field, ensure that the box is checked to enable the rule; uncheck the box to disable the rule.

Symantec Endpoint Protection only processes the rules that you enable. All rules are enabled by default.
- 4 Double-click the **Name** field and type a unique name for the firewall rule.
- 5 Right-click the **Action** field and select the action that you want Symantec Endpoint Protection to take if the rule is triggered.
- 6 In the **Application** field, define an application.
See [“Defining information about applications”](#) on page 356.
- 7 In the **Host** field, specify a host trigger.
See [“Blocking traffic to or from a specific server”](#) on page 373.
- 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 374.
- 9 In the **Service** field, specify a network service trigger.
See [“Controlling whether networked computers can share messages, files, and printing”](#) on page 375.
- 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 377.
- 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 378.
- 13 In the **Time** column, specify the time periods in which this rule is active.
See [“Scheduling when a firewall rule is active”](#) on page 379.

- 14 Right-click the **Screen Saver** field and specify the state that the client computer's screen saver must be in for the rule to be active.

The **Created At** field is not editable. If the policy is shared, the term Shared appears. If the policy is not shared, the field shows the name of the group to which that the non-shared policy is assigned.

- 15 Right-click the **Description** field, click **Edit**, type an optional description for the rule, and then click **OK**.
- 16 If you are done with the configuration of the rule, click **OK**.

See [“Setting up firewall rules”](#) on page 367.

See [“Managing firewall rules”](#) on page 348.

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 Do all of the following tasks:

from the **Type** drop-down list

- 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 [“Setting up firewall rules”](#) on page 367.

See [“Customizing firewall rules”](#) on page 370.

See [“Editing a policy”](#) on page 321.

See [“Adding host groups”](#) on page 362.

Allowing only specific traffic to the local subnet

You can create a firewall rule that permits only specific traffic to your local subnet. This firewall rule always applies to your local subnet IP address, regardless of what the address is. Therefore, even if you change your local subnet IP address, you never have to modify this rule for the new address.

For example, you can create this rule to permit traffic to port 80 only on the local subnet, regardless of what the local subnet IP address is.

To allow only specific traffic to the local subnet

1 In the console, open a Firewall policy.

2 On the **Firewall Policy** page, click **Rules**.

3 On the **Rules** tab, in the **Rules** list, select the rule that you want to edit.

4 In the **Firewall Rules** table, in the **Host** column, double-click on the rule for which you want to create a local subnet traffic condition.

5 Under the type of hosts for which this rule applies (Local or Remote), click **Add**.

6 Click the **Address Type** drop-down list and select **Local Subnet**.

7 Click **OK**, and then click **OK** again to close out of the **Host List** dialog box.

See [“The types of security policies”](#) on page 318.

See [“Editing a policy”](#) on page 321.

See [“Customizing firewall rules”](#) on page 370.

Controlling whether networked computers can share messages, files, and printing

Network services let networked computers send and receive messages, shared files, and print. You can create a firewall rule that allows or blocks network services.

You can add a custom network service through a firewall rule. However, that network service is not added to the default list. You cannot access the custom service from any other rule.

To control whether networked computers can share messages, files, and printing

- 1 In the console, open a Firewall policy.
- 2 On the **Firewall Policy** page, click **Rules**.
- 3 On the **Rules** tab, in the **Rules** list, select the rule you want to edit, right-click the **Service** field, and then click **Edit**.
- 4 In the **Service List** dialog box, check box beside each service that you want to trigger the rule.
- 5 To add an additional service for the selected rule only, click **Add**.
- 6 In the **Protocol** dialog box, select a protocol from the **Protocol** drop-down list.
- 7 Fill out the appropriate fields.
- 8 Click **OK**.
- 9 Click **OK**.
- 10 Click **OK**.

See [“About firewall rule network services triggers”](#) on page 364.

See [“Setting up firewall rules”](#) on page 367.

See [“Adding network services to the default network services list”](#) on page 364.

See [“Editing a policy”](#) on page 321.

See [“Customizing firewall rules”](#) on page 370.

Permitting clients to browse for files and printers in the network

You can enable the client to either share its files or to browse for shared files and printers on the local network. To prevent network-based attacks, you may not want to enable network file and printer sharing.

You enable network file and print sharing by adding firewall rules. The firewall rules allow access to the ports to browse and share files and printers. You create one

firewall rule so that the client can share its files. You create a second firewall rule so that the client can browse for other files and printers.

The settings work differently based on the type of control that you specify for your client, as follows:

Client control or mixed control	Users on the client can enable these settings automatically by configuring them in Network Threat Protection.
Mixed control	A server firewall rule that specifies this type of traffic can override these settings.
Server control	These settings are not available on the client.

To permit clients to browse for files and printers in the network

- 1 In the console, open a Firewall policy.
- 2 On the **Firewall Policy** page, click **Rules**.
- 3 On the **Rules** tab, in the **Rules** list, select the rule you want to edit, right-click the **Service** field, and then click **Edit**.
- 4 In the **Service List** dialog box, click **Add**.
- 5 In the **Protocol** dialog box, in the **Protocol** drop-down list, click **TCP**, and then click **Local/Remote**.
- 6 Do one of the following tasks:

To permit clients to browse for files and printers in the network	In the Remote port drop-down list, type 88, 135, 139, 445 .
To enable other computers to browse files on the client	In the Local Port drop-down list, type 88, 135, 139, 445 .
- 7 Click **OK**.
- 8 In the **Service List** dialog box, click **Add**.
- 9 In the **Protocol** dialog box, in the **Protocol** drop-down list, click **UDP**.

10 Do one of the following tasks:

- | | |
|---|---|
| To permit clients to browse for files and printers in the network | In the Local Port drop-down list, type 137, 138 .
In the Remote Port drop-down list, type 88 . |
| To enable other computers to browse files on the client | In the Local Port drop-down list, type 88, 137, 138 . |

11 Click **OK**.

12 In the **Service List** dialog box, make sure that the two services are enabled, and then click **OK**.

13 On the **Rules** tab, make sure the **Action** field is set to **Allow**.

14 If you are done with the configuration of the policy, click **OK**.

15 If you are prompted, assign the policy to a location.

See [“Setting up firewall rules”](#) on page 367.

See [“Customizing firewall rules”](#) on page 370.

See [“Editing a policy”](#) on page 321.

Setting up notifications for firewall rule violations

You can configure Symantec Endpoint Protection to send you an email message each time the firewall detects a rule violation, attack, or event. For example, you may want to know when a client blocks the traffic that comes from a particular IP address.

To set up notifications for firewall rule violations

- 1** In the console, open a Firewall policy.
- 2** On the **Firewall Policy** page, click **Rules**.
- 3** On the **Rules** tab, select a rule, right-click the **Logging** field, and do one or more of the following tasks:

To send an email message when a firewall rule is triggered	Check Send Email Alert .
--	---------------------------------

To generate a log event when a firewall rule is triggered	Check both Write to Traffic Log and Write to Packet Log .
---	---

- 4 When you are done with the configuration of this policy, click **OK**.
- 5 Configure a security alert.
- 6 Configure a mail server.
- 7 Click **OK**.

See [“Setting up firewall rules”](#) on page 367.

See [“Customizing firewall rules”](#) on page 370.

See [“Setting up administrator notifications”](#) on page 630.

Controlling the traffic that passes through a network adapter

When you define a network adapter trigger, the rule is relevant only to the traffic that the specified adapter transmits or receives.

You can add a custom network adapter from a firewall rule. However, that adapter is not added to the shared list. You cannot access the custom adapter from any other rule.

To control the traffic that passes through a network adapter

- 1 In the console, open a Firewall policy.
- 2 On the **Firewall Policy** page, click **Rules**.
- 3 On the **Rules** tab, in the **Rules** list, select the rule you want to edit, right-click the **Adapter** field, and then click **More Adapters**.
- 4 In the **Network Adapter** dialog box, do one of the following actions:

To trigger the rule for any adapter (even if it is not listed) Click **Apply the rule to all adapters**, and then go to step 7.

To trigger the rule for selected adapters Click **Apply the rule to the following adapters**.

Then check the box beside each adapter that you want to trigger the rule.

- 5 To add a custom adapter for the selected rule only, do the following tasks:
 - Click **Add**.
 - In the **Network Adapter** dialog box, select the adapter type and type the adapter's brand name in the **Adapter Identification** text field.
- 6 Click **OK**.

7 Click **OK**.

8 Click **OK**.

See [“Setting up firewall rules”](#) on page 367.

See [“Customizing firewall rules”](#) on page 370.

See [“Editing a policy”](#) on page 321.

See [“About firewall rule network adapter triggers”](#) on page 365.

Scheduling when a firewall rule is active

You can specify a time period when a firewall rule is active.

To schedule when a firewall rule is active

1 In the console, open a Firewall policy.

2 On the **Firewall Policy** page, click **Rules**.

3 On the **Rules** tab, select the rule you want to edit, right-click the **Time** field, and then click **Edit**.

4 In the **Schedule List** dialog box, click **Add**.

5 In the **Add Schedule** dialog box, configure the start time and end time that you want the rule to be active or not active.

6 In the **Month** drop-down list, select either **All** or a specific month.

7 Check the box for the time frame that you want.

If you check **Specify days**, check one or more of the listed days.

8 Click **OK**.

9 In the **Schedule** list, do one of the following actions:

To keep the rule active during this time Uncheck the box in the **Any Time Except** column.

To make the rule inactive during this time Check the box in the **Any Time Except** column.

10 Click **OK**.

See [“Setting up firewall rules”](#) on page 367.

See [“Customizing firewall rules”](#) on page 370.

See [“Editing a policy”](#) on page 321.

Managing intrusion prevention

This chapter includes the following topics:

- [Managing intrusion prevention on client computers](#)
- [How intrusion prevention works](#)
- [About Symantec IPS signatures](#)
- [About custom IPS signatures](#)
- [Enabling or disabling network intrusion prevention or browser intrusion prevention](#)
- [Creating exceptions for IPS signatures](#)
- [Setting up a list of excluded computers](#)
- [Configuring client intrusion prevention notifications](#)
- [Managing custom intrusion prevention signatures](#)

Managing intrusion prevention on client computers

The default intrusion prevention settings protect client computers against a wide variety of threats. You can change the default settings for your network.

If you run Symantec Endpoint Protection on servers, intrusion prevention might affect server resources or response time. For more information, see the following knowledge base article:

[Best Practices for the Intrusion Prevention System component of Symantec Endpoint Protection on high-availability/high bandwidth servers](#)

Note: The Linux client does not support intrusion prevention.

Table 16-1 Managing intrusion prevention

Task	Description
Learn about intrusion prevention	<p>Learn how intrusion prevention detects and blocks network and browser attacks.</p> <p>See “How intrusion prevention works” on page 383.</p> <p>See “About Symantec IPS signatures” on page 384.</p>
Enable or disable intrusion prevention	<p>You might want to disable intrusion prevention for troubleshooting purposes or if client computers detect excessive false positives. However, to keep your client computers secure, typically you should not disable intrusion prevention.</p> <p>You can enable or disable the following types of intrusion prevention in the Intrusion Prevention policy:</p> <ul style="list-style-type: none"> ■ Network intrusion prevention ■ Browser intrusion prevention (Windows computers only) <p>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.</p> <p>See “Enabling or disabling network intrusion prevention or browser intrusion prevention” on page 386.</p> <p>See “Creating exceptions for IPS signatures” on page 387.</p> <p>You can also enable or disable both types of intrusion prevention, as well as the firewall, when you run the Enable Network Threat Protection or Disable Network Threat Protection command.</p> <p>See “Running commands on client computers from the console” on page 261.</p>

Table 16-1 Managing intrusion prevention (*continued*)

Task	Description
Create exceptions to change the default behavior of Symantec network intrusion prevention signatures	<p>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.</p> <p>Note: You cannot change the behavior of browser intrusion prevention signatures.</p> <p>You might want to change the default behavior of some network signatures for the following reasons:</p> <ul style="list-style-type: none"> ■ 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. <p>See “Creating exceptions for IPS signatures” on page 387.</p> <p>You can use application control to prevent users from running peer-to-peer applications on their computers.</p> <p>See “Typical application control rules” on page 533.</p> <p>If you want to block the ports that send and receive peer-to-peer traffic, use a Firewall policy.</p> <p>See “Creating a firewall policy” on page 339.</p>

Table 16-1 Managing intrusion prevention (*continued*)

Task	Description
<p>Create exceptions to ignore browser signatures on client computers (Windows only)</p>	<p>You can create exceptions to exclude browser signatures from browser intrusion prevention on Windows computers.</p> <p>You might want to ignore browser signatures if browser intrusion prevention causes problems with browsers in your network.</p> <p>See “Creating exceptions for IPS signatures” on page 387.</p>
<p>Exclude specific computers from network intrusion prevention scans</p>	<p>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.</p> <p>When you exclude computers, you also exclude them from the denial of service protection and port scan protection that the firewall provides.</p> <p>See “Setting up a list of excluded computers” on page 389.</p>
<p>Configure intrusion prevention notifications</p>	<p>By default, messages appear on client computers for intrusion attempts. You can customize the message.</p> <p>See “Configuring client intrusion prevention notifications” on page 390.</p>
<p>Create custom intrusion prevention signatures (Windows only)</p>	<p>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.</p> <p>For example, you might want to use custom intrusion prevention signatures to block and log websites.</p> <p>See “Managing custom intrusion prevention signatures” on page 391.</p>
<p>Monitor intrusion prevention</p>	<p>Regularly check that intrusion prevention is enabled on the client computers in your network.</p> <p>See “Monitoring endpoint protection” on page 593.</p>

How intrusion prevention works

Intrusion prevention is part of Network Threat Protection.

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 16-2 Types of intrusion prevention

Type	Description
Network intrusion prevention	<p>Network intrusion prevention uses signatures to identify attacks on client computers. For known attacks, intrusion prevention automatically discards the packets that match the signatures.</p> <p>You can also create your own custom network signatures as part of an Intrusion Prevention policy. You cannot create custom signatures on the client directly; however, you can import custom signatures on the client. Custom signatures are supported on Windows computers only.</p> <p>See “About Symantec IPS signatures” on page 384.</p>
Browser intrusion prevention (Windows only)	<p>Browser intrusion prevention monitors attacks on Internet Explorer and Firefox. Browser intrusion prevention is not supported on any other browsers.</p> <p>Firefox might disable the Symantec Endpoint Protection plug-in, but you can turn it back on.</p> <p>This type of intrusion prevention uses attack signatures as well as heuristics to identify attacks on browsers.</p> <p>For some browser attacks, intrusion prevention requires that the client terminate the browser. A notification appears on the client computer.</p> <p>See the following knowledge base article for the latest information about the browsers that browser intrusion prevention protects: Supported browser versions for browser intrusion prevention.</p>

See [“Managing intrusion prevention on client computers”](#) on page 380.

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 knowledge base article:

[Built-in signatures for Symantec Endpoint Protection IPS for Mac](#)

See [“Creating exceptions for IPS signatures”](#) on page 387.

See [“Managing intrusion prevention on client computers”](#) on page 380.

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 [“Configuring Windows client installation feature sets”](#) on page 127.

Note: Custom signatures are supported on Windows computers only.

See [“Managing custom intrusion prevention signatures”](#) on page 391.

Enabling or disabling network intrusion prevention or browser intrusion prevention

You can enable or disable each type of intrusion prevention separately. 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 Threat Protection** 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.

See [“Creating exceptions for IPS signatures”](#) on page 387.

Browser intrusion prevention is supported on Windows computers only.

See [“Managing intrusion prevention on client computers”](#) on page 380.

You can also exclude particular computers from network intrusion prevention.

See [“Setting up a list of excluded computers”](#) on page 389.

Note: To configure these settings in mixed control, you must also enable these settings in the **Client User Interface Mixed Control Settings** dialog box.

See [“Configuring firewall settings for mixed control”](#) on page 344.

To enable or disable network intrusion prevention or browser intrusion prevention

- 1 In the console, open an Intrusion Prevention policy.
- 2 On the **Intrusion Prevention Policy** page, click **Intrusion Prevention**.
- 3 Check or uncheck the following options:
 - **Enable Network Intrusion Prevention**
 - **Enable Browser Intrusion Prevention for Windows**
- 4 Click the icon to lock or unlock the options on client computers. When you lock an option, you prevent user changes to the option.
- 5 Click **OK**.

Creating exceptions for IPS signatures

You 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 client computers”](#) on page 380.

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 495.

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 and outbound traffic, but only to the source of the traffic.

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 **Intrusion Prevention 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 373.
- 5 To add the hosts that you want to exclude, click **Add**.
- 6 In the **Host** dialog box, in the drop-down list, select one of the following host types:
 - IP address
 - IP range
 - Subnet
- 7 Enter the appropriate information that is associated with the host type you selected.
For more information about these options, click **Help**.
- 8 Click **OK**.

- 9 Repeat **5** and **8** to add additional devices and computers to the list of excluded computers.
- 10 To edit or delete any of the excluded hosts, select a row, and then click **Edit** or **Delete**.
- 11 Click **OK**.
- 12 When you finish configuring the policy, click **OK**.

Configuring client intrusion prevention notifications

By default, notifications appear on client computers when the client detects intrusion protection events. When these notifications are enabled, they display a standard message. You can add customized text to the standard message.

To client configure intrusion prevention notifications

- 1 In the console, click **Clients** and under **Clients**, select a group.
- 2 On the **Policies** tab, under **Location-specific Policies and Settings**, under a location, expand **Location-specific Settings**.
- 3 To the right of **Client User Interface Control Settings**, click **Tasks**, and then click **Edit Settings**.
- 4 In the **Client User Interface Control Settings for *group name*** dialog box, click either **Server control** or **Mixed control**.
- 5 Beside **Mixed control** or **Server control**, click **Customize**.
 If you click **Mixed control**, on the **Client/Server Control Settings tab**, beside **Show/Hide Intrusion Prevention notifications**, click **Server**. Then click the **Client User Interface Settings** tab.
- 6 In the **Client User Interface Settings** dialog box or tab, click **Display Intrusion Prevention notifications**.
- 7 To enable a sound when the notification appears, click **Use sound when notifying users**.
- 8 Click **OK**.
- 9 Click **OK**.

See [“Managing intrusion prevention on client computers”](#) on page 380.

See [“Setting up administrator notifications”](#) on page 630.

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 [“Configuring Windows client installation feature sets”](#) on page 127.

Table 16-3 Managing custom intrusion prevention signatures

Task	Description
Create a custom library with a signature group	<p>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.</p> <p>See “About custom IPS signatures” on page 385.</p> <p>See “Creating a custom IPS library” on page 392.</p>
Add custom IPS signatures to a custom library	<p>You add custom IPS signatures to a signature group in a custom library.</p> <p>See “Adding signatures to a custom IPS library” on page 393.</p>
Assign libraries to client groups	<p>You assign custom libraries to client groups rather than to a location.</p> <p>See “Assigning multiple custom IPS libraries to a group” on page 395.</p>

Table 16-3 Managing custom intrusion prevention signatures (*continued*)

Task	Description
Change the order of signatures	<p>Intrusion prevention uses the first rule match. Symantec Endpoint Protection checks the signatures in the order that they are listed in the signatures list.</p> <p>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:</p> <ul style="list-style-type: none"> ■ Block all traffic on port 80. ■ Allow all traffic on port 80. <p>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.</p> <p>Note: Firewall rules take precedence over intrusion prevention signatures.</p> <p>See “Changing the order of custom IPS signatures” on page 395.</p>
Copy and paste signatures	You can copy and paste signatures between groups and between libraries.
Define variables for signatures	<p>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.</p> <p>See “Defining variables for custom IPS signatures” on page 396.</p>
Test custom signatures	<p>You should test the custom intrusion prevention signatures to make sure that they work.</p> <p>See “Testing custom IPS signatures” on page 397.</p>

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 391.

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 393.

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 391.

To add a custom signature

- 1 Create a custom IPS library.

 See [“Creating a custom IPS library”](#) on page 392.
- 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",
                regexcontent="[Gg][Ee][Tt] .*[Mm][Pp]3 .*"

```

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

```

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 **ieexplore** or **ieexplore.exe**. If you do not specify a file name, any application can trigger the signature.

- 9 Click **OK**.

The added application is enabled by default. If you want to disable the application until a later time, uncheck the check box in the **Enabled** column.

- 10 In the **Action** group box, select the action you want the client to take when the signature detects the event:

Block	Identifies and blocks the event or attack and records it in the Security Log
Allow	Identifies and allows the event or attack and records it in the Security Log

- 11 To record the event or attack in the Packet Log, check **Write to Packet Log**.

- 12 Click **OK**.

The added signature is enabled by default. If you want to disable the signature until a later time, uncheck the check box in the **Enabled** column.

- 13 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 395.

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 391.

To assign multiple custom IPS libraries to a group

- 1 In the console, click **Clients**.
- 2 Under **Clients**, select the group to which you want to assign the custom signatures.
- 3 On the **Policies** tab, under **Location-independent Policies and Settings**, click **Custom Intrusion Prevention**.
- 4 In the **Custom Intrusion Prevention for *group name*** dialog box, check the check box in the **Enabled** column for each custom IPS library you want to assign to that group.
- 5 Click **OK**.

Changing the order of custom IPS signatures

The IPS engine for custom signatures checks the signatures in the order that they are listed in the signatures list. Only one signature is triggered per packet. When a signature matches an inbound traffic packet or outbound traffic packet, the IPS engine stops checking other signatures. So that the IPS engine executes signatures in the correct order, you can change the order of the signatures in the signatures list. If multiple signatures match, move the higher priority signatures to the top.

For example, if you add a signature group to block TCP traffic in both directions on destination port 80, you might add the following signatures:

- Block all traffic on port 80.
- Allow all traffic on port 80.

If the Block all traffic signature is listed first, the Allow all traffic signature is never enacted. If the Allow all traffic signature is listed first, the Block all traffic signature is never enacted, and all HTTP traffic is always allowed.

Note: Firewall rules take precedence over intrusion prevention signatures.

See [“Managing custom intrusion prevention signatures”](#) on page 391.

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 391.

Before you can use the variables in the signature, you must define them. The variables that you define in the custom signature library can then be used in any signature in that library.

You can copy and paste the content from the existing sample variable to start as a basis for creating content.

To define variables for custom IPS signatures

- 1 Create a custom IPS library.
- 2 In the **Custom Intrusion Prevention Signatures** dialog box, click the **Variables** tab.
- 3 Click **Add**.
- 4 In the **Add Variable** dialog box, type a name and optional description for the variable.
- 5 Add a content string for the variable value of up to 255 characters.

When you enter the variable content string, follow the same syntax guidelines that you use for entering values into signature content.

- 6 Click **OK**.

After the variable is added to the table, you can use the variable in any signature in the custom library.

To use variables in custom IPS signatures

- 1 On the **Signatures** tab, add or edit a signature.
- 2 In the **Add Signature** or **Edit Signature** dialog box, in the **Content** field, type the variable name with a dollar sign (\$) in front of it.

For example, if you create a variable named HTTP for specifying HTTP ports, type the following:

\$HTTP

- 3 Click **OK**.
- 4 When you finish configuring this library, click **OK**.

Testing custom IPS signatures

After you create custom IPS signatures, you should test them to make sure that they function correctly.

Table 16-4 Testing custom IPS signatures

Step	Action	Description
Step 1	Make sure that clients use the current Intrusion Prevention policy	The next time that the client receives the policy, the client applies the new custom signatures. See “How the client computer and the management server communicate” on page 169.
Step 2	Test the signature content on the client	You should test the traffic that you want to block on the client computers. For example, if your custom IPS signatures should block MP3 files, try to download some MP3 files to the client computers. If the download does not occur, or times out after many tries, the custom IPS signature is successful. You can click Help for more information about the syntax that you can use in custom IPS signatures.
Step 3	View blocked events in Symantec Endpoint Protection Manager	You can view events in the Network Threat Protection Attack logs. The message you specify in the custom IPS signature appears in the log. See “Monitoring endpoint protection” on page 593.

See [“Managing custom intrusion prevention signatures”](#) on page 391.

Managing Virus and Spyware Protection

This chapter includes the following topics:

- Preventing and handling virus and spyware attacks on client computers
- Remediating risks on the computers in your network
- Managing scans on client computers
- Setting up scheduled scans that run on Windows computers
- Setting up scheduled scans that run on Mac computers
- Setting up scheduled scans that run on Linux computers
- Running on-demand scans on client computers
- Adjusting scans to improve computer performance
- Adjusting scans to increase protection on your client computers
- Managing Download Insight detections
- How Symantec Endpoint Protection uses reputation data to make decisions about files
- How Symantec Endpoint Protection policy features work together on Windows computers
- About submitting information about detections to Symantec Security Response
- About submissions throttling
- Enabling or disabling client submissions to Symantec Security Response

- [Specifying a proxy server for client submissions and other external communications](#)
- [Managing the Quarantine](#)
- [Managing the virus and spyware notifications that appear on client computers](#)
- [About the pop-up notifications that appear on 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 17-1 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 clients and client computers” on page 253.
Keep definitions current	Make sure that the latest definitions are installed on client computers. You can check the definitions date on the Clients tab. You can run a command to update the definitions that are out of date. You can also run a computer status report to check the latest definitions date. See “Managing content updates” on page 181.

Table 17-1 Protecting computers from virus and spyware attacks (*continued*)

Task	Description
Run regular scans	<p>By default, Auto-Protect and SONAR run on client computers. A default scheduled active scan also runs on client computers.</p> <p>You can run scans on demand. You can customize the scan settings.</p> <p>See “Running on-demand scans on client computers” on page 426.</p> <p>You might want to create and customize scheduled scans.</p> <p>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.</p> <p>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.</p> <p>See “Setting up scheduled scans that run on Windows computers” on page 422.</p> <p>See “Setting up scheduled scans that run on Mac computers” on page 424.</p> <p>See “Setting up scheduled scans that run on Linux computers” on page 425.</p>
Let clients upload critical events immediately	<p>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.</p> <p>Administrator notifications can alert you right away when the damper period for relevant notifications is set to None.</p> <p>See “Setting up administrator notifications” on page 630.</p> <p>Note: Only 12.1.4 and newer clients can send critical events immediately. Earlier clients send events at the heartbeat interval only.</p>
Check or modify scan settings for increased protection	<p>By default, virus and spyware scans detect, remove, and repair the side effects of viruses and security risks.</p> <p>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.</p> <p>For example, you might want to increase the Bloodhound™ heuristic protection.</p> <p>You also might want to enable scans of network drives.</p> <p>See “Adjusting scans to increase protection on your client computers” on page 430.</p>

Table 17-1 Protecting computers from virus and spyware attacks (*continued*)

Task	Description
Allow clients to submit information about detections to Symantec	<p>Clients can submit information about detections to Symantec. The submitted information helps Symantec address threats.</p> <p>See “Enabling or disabling client submissions to Symantec Security Response” on page 442.</p>
Run intrusion prevention	<p>Symantec recommends that you run intrusion prevention on your client computers as well as Virus and Spyware Protection.</p> <p>See “Managing intrusion prevention on client computers” on page 380.</p>
Remediate infections if necessary	<p>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.</p> <p>See “Remediating risks on the computers in your network” on page 401.</p>

Remediating risks on the computers in your network

You remediate risks as part of handling virus and spyware attacks on your computers.

You use the Reports and Monitors features in the console to determine what computers are infected and to view the results of remediation.

Table 17-2 Remediating risks on client computers

Step	Task	Description
Step 1	Identify infected and at-risk computers	<p>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.</p> <p>Note: Unremediated SONAR detections are not counted as Still Infected. They are part of the Suspicious count in the summary.</p> <p>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.</p> <p>Files that are considered "still infected" are rescanned when new definitions arrive or as soon as the client computer is idle.</p> <p>See "Identifying the infected and at-risk computers" on page 403.</p>
Step 2	Update definitions and rescan	<p>You should make sure that clients use the latest definitions.</p> <p>For the clients that run on Windows computers, you should also make sure that your scheduled and on-demand scans use the Insight Lookup feature.</p> <p>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.</p> <p>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.</p> <p>See "Managing content updates" on page 181.</p>
Step 3	Check scan actions and rescan	<p>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.</p> <p>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.</p> <p>See "Checking the scan action and rescanning the identified computers" on page 404.</p>
Step 4	Restart computers if necessary to complete remediation	<p>Computers may still be at risk or infected because they need to be restarted to finish the remediation of a virus or security risk.</p> <p>You can view the Risk log to determine if any computers require a restart.</p> <p>You can run a command from the Computer Status log to restart computers.</p> <p>See "Running commands on client computers from the console" on page 261.</p>

Table 17-2 Remediating risks on client computers (*continued*)

Step	Task	Description
Step 5	Investigate and clean remaining risks	<p>If any risks remain, you should investigate them further.</p> <p>You can check the Symantec Security Response webpage for up-to-date information about viruses and security risks.</p> <p>http://securityresponse.symantec.com</p> <p>On the client computer, you can also access the Security Response website from the scan results dialog box.</p> <p>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.</p> <p>See “What you should know before you run Power Eraser from the Symantec Endpoint Protection Manager console” on page 763.</p> <p>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.</p> <p>See “Troubleshooting computer issues with the Symantec Help support tool” on page 744.</p>
Step 6	Check the Computer Status log	<p>View the Computer Status log to make sure that risks are remediated or removed from client computers.</p> <p>See “Viewing logs” on page 613.</p>

For more information, see [Virus removal and troubleshooting on a network](#).

See “[Preventing and handling virus and spyware attacks on client computers](#)” on page 399.

See “[Monitoring endpoint protection](#)” on page 593.

Identifying the infected and at-risk computers

You can use the Symantec Endpoint Protection Manager Home page and a Risk report to identify the computers that are infected and at risk.

To identify infected computers

- 1 In the console, click **Home** and view the Virus and Risks Activity Summary.

If you are a system administrator, you see counts of the number of Newly Infected and Still infected computers in your site. If you are a domain administrator, you see counts of the number of Newly Infected and Still infected computers in your domain.

Still Infected is a subset of Newly Infected, and the Still Infected count goes down as you eliminate the risks from your network. Computers are still infected if a subsequent scan would report them as infected. For example, Symantec Endpoint Protection might have been able to clean a risk only partially from a computer, so Auto-Protect still detects the risk.
- 2 In the console, click **Reports**.
- 3 In the **Report type** list box, click **Risk**.
- 4 In the **Select a report** list box, click **Infected and At Risk Computers**.
- 5 Click **Create Report** and note the lists of the infected and at-risk computers that appear.

See [“Remediating risks on the computers in your network”](#) on page 401.

Checking the scan action and rescanning the identified computers

If you have infected and at-risk computers, you should identify why the computers are still infected or at risk. Check the action that was taken for each risk on the infected and at risk computers. It may be that the action that was configured and taken was Left Alone. If the action was Left Alone, you should either clean the risk from the computer, remove the computer from the network, or accept the risk. For Windows clients, you might want to edit the Virus and Spyware Protection policy and change the scan action.

See [“Remediating risks on the computers in your network”](#) on page 401.

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 478.

If your policy is configured to use Push mode, it is pushed out to the clients in the group at the next heartbeat.

See [“How the client computer and the management server communicate”](#) on page 169.

3 Click **Back**.

4 On the **Logs** tab, select the Computer Status log, and then click **View Log**.

5 If you changed an action and pushed out a new policy, select the computers that need to be rescanned with the new settings.

6 In the **Command** list box, select **Scan**, and then click **Start** to rescan the computers.

You can monitor the status of the Scan command from the **Command Status** tab.

Managing scans on client computers

Some scans run by default, but you might want to change settings or set up your own scheduled scans. You can also customize scans and change how much protection they provide on your client computers.

Table 17-3 Modifying scans on client computers

Task	Description
Review the types of scans and default settings	<p>Check your scan settings. You can review the defaults and determine if you want to make changes.</p> <p>See “About the types of scans and real-time protection” on page 408.</p> <p>See “About the default Virus and Spyware Protection policy scan settings” on page 417.</p>
Create scheduled scans and run on-demand scans	<p>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.</p> <p>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.</p> <p>Note: For managed clients, Symantec Endpoint Protection provides a default scheduled scan that scans all files, folders, and locations on the client computers.</p> <p>See “Setting up scheduled scans that run on Windows computers” on page 422.</p> <p>See “Setting up scheduled scans that run on Mac computers” on page 424.</p> <p>See “Setting up scheduled scans that run on Linux computers” on page 425.</p> <p>See “Running on-demand scans on client computers” on page 426.</p>
Customize scan settings for your environment	<p>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.</p> <p>For scheduled scans, you can also set options for missed scans, randomized scans, and whether to scan network drives.</p> <p>See “Customizing the virus and spyware scans that run on Windows computers” on page 461.</p> <p>See “Customizing the virus and spyware scans that run on Mac computers” on page 462.</p> <p>See “Customizing the virus and spyware scans that run on Linux computers” on page 463.</p>

Table 17-3 Modifying scans on client computers (*continued*)

Task	Description
Adjust scans to improve client computer performance	<p>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.</p> <p>Note: When you adjust settings to optimize client computer performance, you might decrease some security on your client computers.</p> <p>See “Adjusting scans to improve computer performance” on page 427.</p>
Adjust scans to increase protection on your client computers	<p>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.</p> <p>See “Adjusting scans to increase protection on your client computers” on page 430.</p>
Manage Download Insight detections	<p>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.</p> <p>See “Managing Download Insight detections” on page 432.</p>
Manage SONAR	<p>SONAR is part of Proactive Threat Protection on your client computers. However, SONAR settings are part of a Virus and Spyware Protection policy.</p> <p>See “Managing SONAR” on page 486.</p>
Configure exceptions for scans	<p>You can create exceptions for the files and applications that you know are safe. Symantec Endpoint Protection also excludes some files and folders automatically.</p> <p>See “Managing exceptions in Symantec Endpoint Protection” on page 495.</p> <p>See “About the files and folders that Symantec Endpoint Protection excludes from virus and spyware scans” on page 414.</p>
Manage files in the Quarantine	<p>You can monitor and delete the files that are quarantined on your client computers. You can also specify settings for the Quarantine.</p> <p>See “Managing the Quarantine” on page 445.</p>
Allow clients to submit information about detections to Symantec	<p>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.</p> <p>See “Enabling or disabling client submissions to Symantec Security Response” on page 442.</p>

Table 17-3 Modifying scans on client computers (*continued*)

Task	Description
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 450.

About the types of scans and real-time protection

Symantec Endpoint Protection includes different types of scans and real-time protection to detect different types of viruses, threats, and risks.

By default, Symantec Endpoint Protection runs an active scan every day at 12:30 P.M. Symantec Endpoint Protection also runs an active scan when new definitions arrive on the client computer. On unmanaged computers, Symantec Endpoint Protection also includes a default startup scan that is disabled.

Note: When a client computer is off or in hibernation or sleep mode, the computer might miss a scheduled scan. When the computer starts up or wakes, by default the scan is retried within a specified interval. If the interval already expired, Symantec Endpoint Protection does not run the scan and waits until the next scheduled scan time. You can modify the settings for missed scheduled scans.

You should make sure that you run an active scan every day on the computers in your network. You might want to schedule a full scan once a week or once a month if you suspect that you have an inactive threat in your network. Full scans consume more computer resources and might affect computer performance.

See [“Managing scans on client computers”](#) on page 405.

Table 17-4 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. See “About the types of Auto-Protect” on page 410. See “Customizing Auto-Protect for Linux clients” on page 466.

Table 17-4 Scan types (*continued*)

Scan type	Description
<p>Download Insight (Windows only)</p>	<p>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.</p> <p>Download Insight functions as part of Auto-Protect and requires Auto-Protect to be enabled.</p> <p>See “How Symantec Endpoint Protection uses reputation data to make decisions about files” on page 436.</p>
<p>Administrator-defined scans</p>	<p>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.</p> <p>The following types of administrator-defined scans are available:</p> <ul style="list-style-type: none"> ■ 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. <p>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.</p> <p>See “Setting up scheduled scans that run on Windows computers” on page 422.</p> <p>See “Setting up scheduled scans that run on Mac computers” on page 424.</p>

Table 17-4 Scan types (*continued*)

Scan type	Description
SONAR (Windows only)	<p>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.</p> <p>Like proactive threat scans, SONAR detects keyloggers, spyware, and any other application that might be malicious or potentially malicious.</p> <p>Note: SONAR is only supported on Windows computers that run Symantec Endpoint Protection version 12.1 and later.</p> <p>See “About SONAR” on page 484.</p>
Early launch anti-malware (ELAM) (Windows only)	<p>Works with the Windows early launch anti-malware driver. Supported only on Windows 8 and Windows Server 2012.</p> <p>Early launch anti-malware provides protection for the computers in your network when they start up and before third-party drivers initialize.</p> <p>See “Managing early launch anti-malware (ELAM) detections” on page 453.</p>

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 17-5 Types of Auto-Protect

Type of Auto-Protect	Description
Auto-Protect	<p>Continuously scans files as they are read from or written to the client computer.</p> <p>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.</p> <p>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.</p> <p>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.</p>
Internet Email Auto-Protect (Windows only)	<p>Scans inbound Internet email body and email attachments for viruses and security risks; also performs outbound email heuristics scanning.</p> <p>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.</p> <p>Note: For performance reasons, Internet Email Auto-Protect for POP3 is not supported on server operating systems.</p> <p>Email scanning does not support IMAP, AOL, or HTTP-based email such as Hotmail or Yahoo! Mail.</p>

Table 17-5 Types of Auto-Protect (*continued*)

Type of Auto-Protect	Description
<p>Microsoft Outlook Auto-Protect (Windows only)</p>	<p>Downloads incoming Microsoft Outlook email attachments and scans for viruses and security risks when the user reads the message and opens the attachment.</p> <p>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.</p> <p>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.</p> <p>If a user downloads a large attachment over a slow connection, mail performance is affected. You may want to disable this feature for users who regularly receive large attachments.</p> <p>Note: You should not install Microsoft Outlook Auto-Protect on a Microsoft Exchange Server. Instead you should install Symantec Mail Security for Microsoft Exchange.</p>
<p>Lotus Notes Auto-Protect (Windows only)</p>	<p>Scans incoming Lotus Notes email attachments for viruses and security risks.</p> <p>Lotus Notes Auto-Protect supports Lotus Notes 7.x or later.</p> <p>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.</p>

See [“About the types of scans and real-time protection”](#) on page 408.

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 478.

You can view information about specific virus and security risks on the Symantec Security Response Web site.

Table 17-6 Viruses and security risks

Risk	Description
Viruses	<p>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.</p> <p>The following types of threats are included in the virus category:</p> <ul style="list-style-type: none"> ■ Malicious Internet bots Programs that run automated tasks over the Internet. Bots can be used to automate attacks on computers or to collect information from Web sites. ■ Worms Programs that replicate without infecting other programs. Some worms spread by copying themselves from disk to disk, while others replicate in memory to reduce computer performance. ■ Trojan horses Programs that hide themselves in something benign, such as a game or utility. ■ Blended threats Threats that blend the characteristics of viruses, worms, Trojan horses, and code with server and Internet vulnerabilities to initiate, transmit, and spread an attack. Blended threats use multiple methods and techniques to spread rapidly and cause widespread damage. ■ Rootkits Programs that hide themselves from a computer's operating system.
Adware	Programs that deliver any advertising content.
Dialers	Programs that use a computer, without the user's permission or knowledge, to dial out through the Internet to a 900 number or FTP site. Typically, these numbers are dialed to accrue charges.
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 17-6 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 17-7 File and folder exclusions

Files	Description
Microsoft Exchange	<p>The client software automatically creates file and folder scan exclusions for the following Microsoft Exchange Server versions:</p> <ul style="list-style-type: none"> ■ Exchange 5.5 ■ Exchange 6.0 ■ Exchange 2000 ■ Exchange 2003 ■ Exchange 2007 ■ Exchange 2007 SP1 ■ Exchange 2010 <p>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.</p> <p>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.</p> <p>For more information, see the knowledge base article, Preventing Symantec Endpoint Protection from scanning the Microsoft Exchange 2007 directory structure.</p>

Table 17-7 File and folder exclusions (*continued*)

Files	Description
Microsoft Forefront	<p>The client automatically creates file and folder exclusions for the following Microsoft Forefront products:</p> <ul style="list-style-type: none"> ■ Forefront Server Security for Exchange ■ Forefront Server Security for SharePoint ■ Forefront Threat Management Gateway <p>Check the Microsoft Web site for a list of recommended exclusions.</p> <p>Also see the Symantec Technical Support knowledge base article, Configuring Symantec Endpoint Protection exclusions for Microsoft Forefront.</p>
Active Directory domain controller	<p>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.</p>
Symantec products	<p>The client automatically creates appropriate file and folder scan exclusions for certain Symantec products when they are detected.</p> <p>The client creates exclusions for the following Symantec products:</p> <ul style="list-style-type: none"> ■ 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

Table 17-7 File and folder exclusions (*continued*)

Files	Description
Selected extensions and Microsoft folders	<p>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.</p> <p>For executable files and Microsoft Office files, Auto-Protect can determine a file's type even if a virus changes the file's extension.</p> <p>By default Symantec Endpoint Protection scans all extensions and folders. Any extensions or folders that you deselect are excluded from that particular scan.</p> <p>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.</p> <p>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.</p>
File and folder exceptions	<p>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.</p> <p>Note: By default, users on client computers can also create file and folder exceptions.</p> <p>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.</p>
Trusted files	<p>Virus and spyware scans include a feature that is called Insight that lets scans skip trusted files. You can choose the level of trust for the files that you want to skip, or you can disable the option. If you disable the option, you might increase scan time.</p> <p>Auto-Protect can also skip the files that are accessed by trusted processes such as Windows Search.</p>

See [“Excluding a file or a folder from scans”](#) on page 503.

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 17-8 Virus and Spyware Protection Balanced policy scan settings

Setting	Description
Auto-Protect for the file system	<p>Enabled</p> <p>Download Insight malicious file sensitivity is set to level 5.</p> <p>The Download Insight action for unproven files is Ignore.</p> <p>Auto-Protect includes the following settings:</p> <ul style="list-style-type: none"> ■ 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	<p>Enabled</p> <p>Other types of Auto-Protect include the following settings:</p> <ul style="list-style-type: none"> ■ 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.

Table 17-8 Virus and Spyware Protection Balanced policy scan settings
(continued)

Setting	Description
SONAR	<p>Enabled for Symantec Endpoint Protection 12.1 clients and later. Legacy clients use TruScan settings. TruScan is enabled when SONAR is enabled.</p> <ul style="list-style-type: none"> ■ 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.
Administrator-defined scans	<p>The scheduled scan includes the following default settings:</p> <ul style="list-style-type: none"> ■ Performs an active scan every day at 12:30 P.M. The scan is randomized. ■ Scans all files and folders, including the files that are contained in compressed files. ■ Scans memory, common infection locations, and known virus and security risk locations. ■ Cleans the virus-infected files. Backs up the files before it repairs them. Quarantines the files that cannot be cleaned. ■ Quarantines the files with security risks. Logs the files that cannot be quarantined. ■ Retries missed scans within three days. ■ Insight Lookup is set to level 5. <p>The on-demand scan provides the following protection:</p> <ul style="list-style-type: none"> ■ 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 17-9 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: <ul style="list-style-type: none"> Blocks any system change events.
Global settings	Bloodhound is set to Aggressive.

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

Table 17-10 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: <ul style="list-style-type: none"> Download Insight malicious file sensitivity is set to level 1.
Internet Email Auto-Protect Microsoft Outlook Auto-Protect Lotus Notes Auto-Protect	Disabled
SONAR	Same as Virus and Spyware Protection policy with the following changes: <ul style="list-style-type: none"> Ignores any system change events. Ignores any behavioral policy enforcement events.
Administrator-defined scans	Same as Virus and Spyware Protection policy except the following setting: <ul style="list-style-type: none"> Insight Lookup is set to level 1.

How Symantec Endpoint Protection handles detections of viruses and security risks

Symantec Endpoint Protection uses default actions to handle the detection of viruses and security risks. You can change some of the defaults.

Table 17-11 How Symantec Endpoint Protection handles the detection of viruses and security risks

Detection	Description
Viruses	<p>By default, the Symantec Endpoint Protection client first tries to clean a file that a virus infects.</p> <p>If the client software cannot clean the file, it does the following actions:</p> <ul style="list-style-type: none"> ■ Moves the file to the Quarantine on the infected computer ■ Denies any access to the file ■ Logs the event
Security risks	<p>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.</p> <p>If a security risk cannot be quarantined and repaired, the second action is to log the risk.</p> <p>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.</p> <p>On Windows clients and Linux clients, you can disable Auto-Protect scanning for security risks. You might want to temporarily disable Auto-Protect scanning of security risks if detection of a security risk could compromise a computer's stability. Scheduled and on-demand scans continue to detect the risk.</p>

Detections by SONAR are considered suspicious events. You configure actions for these detections as part of the SONAR configuration.

See [“Managing SONAR”](#) on page 486.

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: 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”](#) on page 445.

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 452.

See [“How Symantec Endpoint Protection handles detections of viruses and security risks”](#) on page 421.

Setting up scheduled scans that run on Windows computers

You configure scheduled scans as part of a Virus and Spyware Protection policy.

Note: Windows settings include some options that are not available for clients that run on other operating systems.

See [“Managing scans on client computers”](#) on page 405.

See [“Customizing administrator-defined scans for clients that run on Windows computers”](#) on page 469.

See [“Excluding file extensions from virus and spyware scans on Windows clients and Linux clients”](#) on page 506.

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	<p>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.</p> <p>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.</p> <p>In either case, if you randomize the scan start time you might change the last run time of the scan.</p>

You can click Help for more information about the options that are used in this procedure.

To set up scheduled scans that run on Windows computers

- 1 In the console, open a Virus and Spyware Protection policy.
- 2 Under **Windows Settings**, click **Administrator-defined Scans**.
- 3 On the **Scans** tab, under **Scheduled Scans**, click **Add**.
- 4 In the **Add Scheduled Scan** dialog box, click **Create a new scheduled scan**.
- 5 Click **OK**.
- 6 In the **Add Scheduled Scan** dialog box, on the **Scan Details** tab, type a name and description for this scheduled scan.
- 7 Click **Active Scan**, **Full Scan**, or **Custom Scan**.
- 8 If you selected **Custom**, under **Scanning**, you can specify the folders to scan.
- 9 Under **File types**, click **Scan all files** or **Scan only selected extensions**.

Note: Scheduled scans always scan container files unless you disable the **Scan files inside compressed files** option under **Advanced Scanning Options** or you create specific exceptions for the container file extensions.

- 10 Under **Enhance the scan by checking**, check or uncheck **Memory**, **Common infection locations**, or **Well-known virus and security risk locations**.
- 11 On the **Schedule** tab, under **Scanning schedule**, set the frequency and the time at which the scan should run.

The retry setting under **Missed Scheduled Scans** changes automatically according to whether you select **Daily**, **Weekly**, or **Monthly**.
- 12 Under **Missed Scheduled Scans**, you can disable the option to run a missed scan or you can change the retry interval.

You can also specify a maximum scan duration before the scan pauses. You can also randomize scan start time.
- 13 If you want to save this scan as a template, check **Save a copy as a Scheduled Scan Template**.
- 14 Click **OK**.

Setting up scheduled scans that run on Mac computers

You configure scheduled scans as part of a Virus and Spyware Protection policy.

See [“Managing scans on client computers”](#) on page 405.

See [“Customizing administrator-defined scans for clients that run on Mac computers”](#) on page 470.

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 405.

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 an on-demand scan on client computers

- 1 In the Symantec Endpoint Protection Manager console, click **Clients**.
- 2 Under **Clients**, right-click the clients or the group that you want to scan.
- 3 Do one of the following actions:
 - Click **Run a command on the group > Scan**.
 - Click **Run Command on Computers > Scan**.
- 4 For Windows clients, select **Active Scan**, **Full Scan**, or **Custom Scan**, and then click **OK**.

See [“Managing scans on client computers”](#) on page 405.

See [“Preventing and handling virus and spyware attacks on client computers”](#) on page 399.

See [“Running commands on client computers from the console”](#) on page 261.

See [“About commands that you can run on client computers”](#) on page 258.

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 17-12 To adjust scans to improve computer performance on Windows computers

Task	Description
<p>Modify tuning and compressed files options for scheduled and on-demand scans</p>	<p>You can adjust the following options for scheduled and on-demand scans:</p> <ul style="list-style-type: none"> ■ 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. <p>See “Customizing administrator-defined scans for clients that run on Windows computers” on page 469.</p>
<p>Use resumable scans</p>	<p>For computers in your network that have large volumes, scheduled scans can be configured as resumable scans.</p> <p>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.</p> <p>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.</p> <p>See “Setting up scheduled scans that run on Windows computers” on page 422.</p>
<p>Adjust Auto-Protect settings</p>	<p>You can adjust some settings for Auto-Protect scans of the file system that might improve your client computers' performance.</p> <p>You can set the following options:</p> <ul style="list-style-type: none"> ■ 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. <p>See “Customizing Auto-Protect for Windows clients” on page 464.</p>

Table 17-12 To adjust scans to improve computer performance on Windows computers *(continued)*

Task	Description
Allow all scans to skip trusted files	<p>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:</p> <ul style="list-style-type: none"> ■ 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. <p>See “Modifying global scan settings for Windows clients” on page 474.</p>
Randomize scheduled scans	<p>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.</p> <p>You can randomize scans to limit the impact on your server.</p> <p>See “Randomizing scans to improve computer performance in virtualized environments on Windows clients” on page 473.</p>
Use Shared Insight Cache in virtualized environments	<p>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 clients computers. Shared Insight Cache is a separate application that you install on a server or in a virtual environment.</p> <p>See “Enabling or disabling the use of a network-based Shared Insight Cache” on page 643.</p>
Disable early launch anti-malware (ELAM) detection	<p>Symantec Endpoint Protection ELAM works with Windows ELAM to provide protection against malicious startup drivers.</p> <p>See “Managing early launch anti-malware (ELAM) detections” on page 453.</p>

Table 17-13 To adjust scans to improve computer performance on Mac computers

Task	Description
Enable idle-time scan	<p>Applies to scheduled scans on clients that run on Mac computers.</p> <p>This option configures scheduled scans to run only while the computer is idle.</p> <p>See “Customizing administrator-defined scans for clients that run on Mac computers” on page 470.</p>

Table 17-13 To adjust scans to improve computer performance on Mac computers (*continued*)

Task	Description
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 465.

Table 17-14 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.
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 405.

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 17-15 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.
Modify settings for administrator-defined scans	<p>You should check or modify the following options:</p> <ul style="list-style-type: none"> ■ Scan performance Set the scan tuning to Best Scan Performance. The setting, however, might affect your client computer performance. Scans run even if the computer is not idle. ■ Scheduled scan duration By default, scheduled scans run until the specified time interval expires and then resume when the client computer is idle. You can set the scan duration to Scan until finished. ■ Use Insight Lookup Insight Lookup uses the latest definition set from the cloud and information from the Insight reputation database to scan and make decisions about files. You should make sure that Insight Lookup is enabled. Insight Lookup settings are similar to the settings for Download Insight. <p>See “Customizing administrator-defined scans for clients that run on Windows computers” on page 469.</p>
Specify stronger scan detection actions	<p>Specify Quarantine, Delete, or Terminate actions for detections.</p> <p>Note: Be careful when you use Delete or Terminate for security risk detections. The action might cause some legitimate applications to lose functionality.</p> <p>See “Changing the action that Symantec Endpoint Protection takes when it makes a detection” on page 478.</p>
Increase the level of Bloodhound protection	<p>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.</p> <p>See “Modifying global scan settings for Windows clients” on page 474.</p>
Adjust Auto-Protect settings	<p>You can change the following options:</p> <ul style="list-style-type: none"> ■ File cache You can disable the file cache so that Auto-Protect rescans good files. ■ Network settings By default, files on network drives are scanned only when they are executed. You can disable this option. <p>See “Customizing Auto-Protect for Windows clients” on page 464.</p>

Table 17-16 Adjusting scans to increase protection on Mac and Linux computers

Task	Description
Modify compressed file options for scans	<p>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.</p> <p>See “Customizing administrator-defined scans for clients that run on Mac computers” on page 470.</p> <p>See “Customizing administrator-defined scans for clients that run on Linux computers” on page 472.</p>
Lock Auto-Protect settings	<p>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.</p> <p>See “Customizing Auto-Protect for Mac clients” on page 465.</p> <p>See “Customizing Auto-Protect for Linux clients” on page 466.</p>
Specify stronger scan detection actions	<p>Specify Quarantine or Delete (Linux only) actions for detections.</p> <p>Note: Be careful when you use Delete for security risk detections. The action might cause some legitimate applications to lose functionality.</p> <p>See “Changing the action that Symantec Endpoint Protection takes when it makes a detection” on page 478.</p>

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 405.

Table 17-17 Managing Download Insight detections

Task	Description
<p>Learn how Download Insight uses reputation data to make decisions about files</p>	<p>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.</p> <p>See “How Symantec Endpoint Protection uses reputation data to make decisions about files” on page 436.</p>
<p>View the Download Risk Distribution report to view Download Insight detections</p>	<p>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.</p> <p>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.</p> <p>The user-allowed files that appear in the report might indicate false positive detections.</p> <p>You can also specify that you receive email notifications about new user-allowed downloads.</p> <p>See “Setting up administrator notifications” on page 630.</p> <p>Users can allow files by responding to notifications that appear for detections.</p> <p>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.</p> <p>See “Running and customizing quick reports” on page 606.</p>

Table 17-17 Managing Download Insight detections (*continued*)

Task	Description
<p>Create exceptions for specific files or Web domains</p>	<p>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.</p> <p>See “Specifying how Symantec Endpoint Protection handles monitored applications on Windows clients” on page 507.</p> <p>See “Excluding a trusted Web domain from scans on Windows clients” on page 508.</p> <p>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.</p> <p>For information about the recommended exceptions, see the following related knowledge base articles:</p> <ul style="list-style-type: none"> ■ 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 <p>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.</p> <p>Symantec Endpoint Protection checks for updates to the Internet Options trusted sites list at user logon and every four hours.</p> <p>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.</p>
<p>Make sure that Insight lookups are enabled</p>	<p>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.</p> <p>See “Enabling or disabling client submissions to Symantec Security Response” on page 442.</p>

Table 17-17 Managing Download Insight detections (*continued*)

Task	Description
<p>Customize Download Insight settings</p>	<p>You might want to customize Download Insight settings for the following reasons:</p> <ul style="list-style-type: none"> ■ 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. <p>Note: If users allow a quarantined file, the file does not automatically run. The user can run the file from the temporary Internet folder. Typically, the folder location is <i>Drive:\Users\username\AppData\Local\Microsoft\Windows\Temporary Internet Files</i>, <i>Drive:\Users\username\AppData\Local\Microsoft\Windows\NetCache</i>, or <i>Drive:\Documents and Settings\username\Local Settings\Temporary Internet Files</i>.</p> <p>See “Customizing Download Insight settings” on page 477.</p>

Table 17-17 Managing Download Insight detections (*continued*)

Task	Description
Allow clients to submit information about reputation detections to Symantec	<p>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.</p> <p>See “Enabling or disabling client submissions to Symantec Security Response” on page 442.</p>

How Symantec Endpoint Protection uses reputation data to make decisions about files

Symantec collects information about files from its global community of millions of users and its Global Intelligence Network. The collected information forms a reputation database that Symantec hosts. Symantec products leverage the information to protect client computers from new, targeted, and mutating threats. The data is sometimes referred to as being in the cloud since it does not reside on the client computer. The client computer must request or query the reputation database.

Symantec uses a technology it calls Insight to determine each file's level of risk or security rating.

Insight determines a file's security rating by examining the following characteristics of the file and its context:

- The source of the file
- How new the file is
- How common the file is in the community
- Other security metrics, such as how the file might be associated with malware

Scanning features in Symantec Endpoint Protection leverage Insight to make decisions about files and applications. Virus and Spyware Protection includes a feature that is called Download Insight. Download Insight relies on reputation information to make detections. If you disable Insight lookups, Download Insight runs but cannot make detections. Other protection features, such as Insight Lookup and SONAR, also use reputation information to make detections; however, those features can use other technologies to make detections.

By default, a client computer sends information about reputation detections to Symantec Security Response for analysis. The information helps to refine Insight's

How Symantec Endpoint Protection policy features work together on Windows computers

reputation database. The more clients that submit information the more useful the reputation database becomes.

You can disable the submission of reputation information. Symantec recommends, however, that you keep submissions enabled.

Client computers also submit other types of information about detections to Symantec Security Response.

See [“Managing Download Insight detections”](#) on page 432.

See [“How Symantec Endpoint Protection policy features work together on Windows computers”](#) on page 437.

See [“Enabling or disabling client submissions to Symantec Security Response”](#) on page 442.

See [“Configuring a site to use a private Insight server for reputation queries”](#) on page 456.

How Symantec Endpoint Protection policy features work together on Windows computers

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 17-18 How policy features work together on Windows computers

Feature	Interoperability Notes
Download Protection	<p>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.</p> <p>If you install Symantec Endpoint Protection without Download Protection, Download Insight has limited capability. Browser Intrusion Prevention and SONAR require Download Protection.</p> <p>The Automatically trust any file downloaded from an intranet website option also requires Download Protection.</p>

How Symantec Endpoint Protection policy features work together on Windows computers

Table 17-18 How policy features work together on Windows computers
(continued)

Feature	Interoperability Notes
Download Insight	<p>Download Insight has the following dependencies:</p> <ul style="list-style-type: none"> ■ 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. <p>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.</p> <p>Even if you disable Download Insight, the Automatically trust any file downloaded from an intranet website option continues to function for Insight Lookup.</p> <p>See “Managing Download Insight detections” on page 432.</p>
Insight Lookup	<p>Uses Insight lookups</p> <p>Insight Lookup uses the latest definitions from the cloud and the Insight reputation database to make decisions about files. If you disable Insight lookups, Insight Lookup uses the latest definitions only to make decisions about files.</p> <p>Insight Lookup also uses the Automatically trust any file downloaded from an intranet website option.</p> <p>Insight Lookup does not run on right-click scans of folders or drives on your client computers. However, Insight Lookup runs on right-click scans of selected files.</p> <p>Note: Insight Lookup uses the configured Insight Lookup slider level value to evaluate the files that were downloaded from a supported portal. If the files were not downloaded from a supported portal, then Insight Lookup detects them only if they have the worst reputation (similar to level 1).</p>

How Symantec Endpoint Protection policy features work together on Windows computers

Table 17-18 How policy features work together on Windows computers
(continued)

Feature	Interoperability Notes
SONAR	<p>SONAR has the following dependencies:</p> <ul style="list-style-type: none"> ■ 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. <p>See "Managing SONAR" on page 486.</p>
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	<p>Uses the firewall.</p> <p>See "Managing custom intrusion prevention signatures" on page 391.</p>
Power Eraser	<p>Uses Insight lookups.</p> <p>Power Eraser uses reputation information to examine files. Power Eraser has a default reputation sensitivity setting that you cannot modify. If you disable the submissions 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.</p> <p>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.</p> <p>See "What you should know before you run Power Eraser from the Symantec Endpoint Protection Manager console" on page 763.</p>

See ["Configuring Windows client installation feature sets"](#) on page 127.

About submitting information about detections to Symantec Security Response

You can configure your client computers to automatically submit information about detections to Symantec Security Response for analysis.

Symantec Response and the Global Intelligence Network use this submitted information to quickly formulate responses to new and developing security threats. The data that you submit improves Symantec's ability to respond to threats and customize protection. Symantec recommends that you always allow submissions.

See [“How Symantec Endpoint Protection uses layers to protect computers”](#) on page 36.

You can choose to submit any of the following types of data:

- File reputation (Windows only)
Information about the files that are detected based on their reputation. The information about these files contributes to the Symantec Insight reputation database to help protect your computers from new and emerging risks.
- Antivirus detections (Windows and Mac only)
Information about virus and spyware scan detections.
- Antivirus advanced heuristic detections (Windows only)
Information about potential threats that are detected by Bloodhound and other virus and spyware scan heuristics.
These detections are silent detections that do not appear in the Risk log. Information about these detections is used for statistical analysis.
- SONAR detections (Windows only)
Information about threats that SONAR detects, which include high or low risk detections, system change events, and suspicious behavior from trusted applications.
- SONAR heuristics (Windows only)
SONAR heuristic detections are silent detections that do not appear in the Risk log. This information is used for statistical analysis.

On the client, you can also manually submit a sample to Response from the Quarantine or through the Symantec Web site. To submit a file through the Symantec Web site, contact Symantec Technical Support.

On Mac clients, you can also disable IPS ping submissions.

[How to disable IPS data submission on Symantec Endpoint Protection for Mac clients](#)

See [“Enabling or disabling client submissions to Symantec Security Response”](#) on page 442.

See [“How Symantec Endpoint Protection uses reputation data to make decisions about files”](#) on page 436.

See [“About submissions throttling”](#) on page 441.

About submissions throttling

Symantec Endpoint Protection throttles client computer submissions to minimize any effect on your network. Symantec Endpoint Protection throttles submissions in the following ways:

- Client computers only send samples when the computer is idle. Idle submission helps randomize the submissions traffic across the network.
- Client computers send samples for unique files only. If Symantec has already seen the file, the client computer does not send the information.
- Symantec Endpoint Protection uses a Submission Control Data (SCD) file. Symantec publishes the SCD file and includes it as part of a LiveUpdate package. Each Symantec product has its own SCD file.

The SCD file controls the following settings:

- How many submissions a client can submit in one day
- How long to wait before the client software retries submissions
- How many times to retry failed submissions
- Which IP address of the Symantec Security Response server receives the submission

If the SCD file becomes out-of-date, then clients stop sending submissions. Symantec considers the SCD file out-of-date when a client computer has not retrieved LiveUpdate content in 7 days. The client stops sending submissions after 14 days.

If clients stop the transmission of the submissions, the client software does not collect the submission information and send it later. When clients start to transmit submissions again, they only send the information about the events that occur after the transmission restart.

See [“About submitting information about detections to Symantec Security Response”](#) on page 440.

Enabling or disabling client submissions to Symantec Security Response

Symantec Endpoint Protection can protect computers by submitting information about detections to Symantec Security Response. Symantec Security Response uses this information to address new and changing threats. Any data you submit improves Symantec's ability to respond to threats and customize protection for your computers. Symantec recommends that you choose to submit as much detection information as possible.

Client computers submit information anonymously about detections. You can specify the types of detections for which clients submit information. You can also enable or disable submissions from client computers. Symantec recommends that you always enable submissions. In some cases, however, you might want to prevent your clients from submitting such information. For example, your corporate policies might prevent your client computers from sending any network information to outside entities.

To enable or disable client submissions to Symantec Security Response

- 1 In the console, select **Clients** then click the **Policies** tab.
- 2 In the **Settings** pane, click **External Communications Settings**.
- 3 Click the **Submissions** tab.
- 4 If you want to enable your client computers to submit data for analysis, check **Let computers automatically forward selected anonymous security information to Symantec**.
- 5 To disable submissions for the client, uncheck **Let computers automatically forward selected anonymous security information to Symantec**.

If you disable submissions for a client and lock the settings, the user is unable to configure the client to send submissions. If you enable, select your submissions types and lock the settings, the user is not able to change your chosen settings. If you do not lock your settings, the user can change the configuration as desired.

Symantec recommends that you submit threat information to help Symantec provide custom threat protection. You may need however, to disable this feature in response to network bandwidth issues or a restriction on data leaving the client. You can check the Client Activity to view log submissions activity if you need to monitor your bandwidth usage.

See [“Viewing logs”](#) on page 613.

- 6 Select the types of information to submit:

- File reputation (Windows only)
Information about files that are detected based on their reputation. The information about these files contributes to the Symantec Insight reputation database to help protect your computers from new and emerging risks.

Note: Unmanaged clients require a paid license to enable the submission of file reputation data.

See [“Licensing an unmanaged Windows client”](#) on page 105.

- Antivirus detections (Windows and Mac only)
Information about virus and spyware scan detections.
 - Antivirus advanced heuristic detections (Windows only)
Information about the potential threats that are detected by Bloodhound and other virus and spyware scan heuristics.
These detections are the silent detections that do not appear in the Risk log. Information about these detections is used for statistical analysis.
 - SONAR detections (Windows only)
Information about the threats that SONAR detects, which include high or low risk detections, system change events, and suspicious behavior from trusted applications.
 - SONAR heuristics (Windows only)
SONAR heuristic detections are silent detections that do not appear in the Risk log. This information is used for statistical analysis.
- 7** Check **Allow Insight lookups for threat detection** to allow Symantec Endpoint Protection to use the Symantec Insight reputation database to make decisions about threats. The option applies to Windows computers only.

Insight lookups are enabled by default. You can disable this option if you do not want to allow Symantec Endpoint Protection to query the Symantec Insight reputation database.

Download Insight, Insight Lookup, and SONAR use Insight lookups for threat detection. Symantec recommends that you allow Insight lookups. Disabling lookups disables Download Insight and may impair the functionality of SONAR heuristics and Insight Lookup.

See [“About submitting information about detections to Symantec Security Response”](#) on page 440.

See [“How Symantec Endpoint Protection uses reputation data to make decisions about files”](#) on page 436.

See “[Specifying a proxy server for client submissions and other external communications](#)” on page 444.

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 knowledge base articles:

- [How to test connectivity to Insight and Symantec licensing servers](#)

- [Required exclusions for proxy servers to allow Symantec Endpoint Protection to connect to Symantec reputation and licensing servers](#)

See [“Enabling or disabling client submissions to Symantec Security Response”](#) on page 442.

See [“Creating exceptions for Virus and Spyware scans”](#) on page 498.

Managing the Quarantine

When virus and spyware scans detect a threat or SONAR detects a threat, Symantec Endpoint Protection places the files in the client computer's local Quarantine.

See [“Managing scans on client computers”](#) on page 405.

Table 17-19 Managing the Quarantine

Task	Description
Monitor files in the Quarantine	<p>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.</p> <p>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.</p>
Delete files in the Quarantine	<p>You can delete a quarantined file if a backup exists or if you have a copy of the file from a trustworthy source.</p> <p>You can delete a quarantined file directly on the infected computer, or by using the Risk log in the Symantec Endpoint Protection console.</p> <p>See “Using the Risk log to delete quarantined files on your client computers” on page 449.</p>
Configure how Symantec Endpoint Protection rescans items in the Quarantine when new definitions arrive	<p>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.</p> <p>See “Configuring how the Quarantine handles the rescanning of files after new definitions arrive” on page 448.</p>

Table 17-19 Managing the Quarantine (*continued*)

Task	Description
<p>Specify how clients submit information about quarantined items</p>	<p>Symantec Endpoint Protection lets users submit infected or suspicious files and related side effects to Symantec Security Response for further analysis. When users submit information, Symantec can refine its detection and repair.</p> <p>You can enable signature-based detections in Quarantine to be forwarded from the local Quarantine to a Central Quarantine Server. Reputation detections in the local Quarantine cannot be sent to a Central Quarantine Server. You can configure the client to forward items if you use a Central Quarantine Server in your security network. The Central Quarantine Server can send the information to Symantec Security Response. Information that clients submit helps Symantec determine if a detected threat is real.</p> <p>Files that are submitted to Symantec Security Response become the property of Symantec Corporation. In some cases, files may be shared with the antivirus community. If Symantec shares files, Symantec uses industry-standard encryption and may make data anonymous to help protect the integrity of the content and your privacy.</p> <p>See “Configuring clients to submit quarantined items to a Central Quarantine Server or Symantec Security Response” on page 448.</p>
<p>Manage the storage of quarantined files</p>	<p>By default, the Quarantine stores backup, repaired, and quarantined files in a default folder. It automatically deletes files after 30 days.</p> <p>You can manage the storage of quarantined items in the following ways:</p> <ul style="list-style-type: none"> ■ 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 446. ■ 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 447.

Specifying a local Quarantine folder

If you do not want to use the default quarantine folder to store quarantined files on client computers, you can specify a different local folder. You can use path expansion by using the percent sign when you type the path. For example, you can type %COMMON_APPDATA%. Relative paths are not allowed.

See [“Managing the Quarantine”](#) on page 445.

To specify a local Quarantine folder

- 1 On the **Virus and Spyware Protection Policy** page, under **Windows Settings**, click **Quarantine**.
- 2 On the **Miscellaneous** tab, under **Local Quarantine Options**, click **Specify the quarantine folder**.
- 3 In the text box, type the name of a local folder on the client computers. You can use path expansion by using the percent sign when typing in the path. For example, you can type %COMMON_APPDATA%, but relative paths are not allowed.
- 4 If you are finished with the configuration for this policy, click **OK**.

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. These options are in the **Windows Settings** menu.

You can use one of the settings, or you can use both together. If you set both types of limits, then all files older than the time you have set are purged first. If the size of the folder still exceeds the size limit that you set, then the oldest files are deleted one by one. The files are deleted until the folder size falls below the specified limit.

See [“Managing the Quarantine”](#) on page 445.

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, under **Repaired files**, check or uncheck **Enable automatic deleting of repaired files**.
- 3 In the **Delete after** box, type a value or click an arrow to select the time interval in days.
- 4 Check **Delete oldest files to limit folder size at**, and then type in the maximum folder size, in megabytes. The default setting is 50 MB.
- 5 Under **Backup Files**, check or uncheck **Enable automatic deleting of backup files**.
- 6 In the **Delete after** box, type or click an arrow to select the time interval in days.

- 7 Check **Delete oldest files to limit folder size at**, and then type the maximum folder size, in megabytes. The default is 50 MB.
- 8 Under **Quarantined Files**, check or uncheck **Enable automatic deleting of quarantined files that could not be repaired**.
- 9 In the **Delete after** box, type a value or click an arrow to select the time interval in days.
- 10 Check **Delete oldest files to limit folder size at**, and then type in the maximum folder size, in megabytes. The default is 50 MB.
- 11 If you are finished with the configuration for this policy, click **OK**.

Configuring clients to submit quarantined items to a Central Quarantine Server or Symantec Security Response

In Symantec Endpoint Protection, you can configure clients to automatically submit quarantine items to a Central Quarantine Server.

You can also let users on the client computers manually submit quarantine items directly to Symantec Security Response.

To configure clients to submit quarantined items to a Central Quarantine Server or Symantec Security Response

- 1 In the console, open a Virus and Spyware Protection policy and under **Windows Settings**, click **Quarantine**.
- 2 Under **Quarantined Items**, do one or both of the following actions:
 - Check **Allow client computers to automatically submit quarantined items to a Quarantine Server**.
Type the fully qualified domain name or IP address of the Quarantine Server.
Type the port number to use, and then select the number of seconds to retry connecting.
 - Check **Allow client computers to manually submit quarantined items to Symantec Security Response**.
- 3 Click **OK**.

See [“Managing the Quarantine”](#) on page 445.

Configuring how the Quarantine handles the rescanning of files after new definitions arrive

You can configure the actions that you want to take when new definitions arrive on client computers. By default, the client rescans items in the Quarantine and

automatically repairs and restores items silently. Typically, you should always use this setting.

If you created an exception for a file or application in the Quarantine, Symantec Endpoint Protection restores the file after new definitions arrive.

See [“Managing the Quarantine”](#) on page 445.

See [“Remediating risks on the computers in your network”](#) on page 401.

To configure how the Quarantine handles the rescanning of files after new definitions arrive

- 1 In the console, open a Virus and Spyware Protection policy and click **Quarantine**.
- 2 On the **General** tab, under **When New Virus Definitions Arrive**, click one of the following options:
 - **Automatically repair and restore files in Quarantine silently**
 - **Repair files in Quarantine silently without restoring**
 - **Prompt user**
 - **Do nothing**
- 3 If you are finished with the configuration for this policy, click **OK**.

Using the Risk log to delete quarantined files on your client computers

You can use the Risk log in the Symantec Endpoint Protection Manager console to delete quarantined files on your client computers. You run the **Delete from Quarantine** command from the log for any quarantined file that you want to delete.

See [“Managing scans on client computers”](#) on page 405.

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.

Managing the virus and spyware notifications that appear on client computers

You must have all entries in the compressed file in the log view. You can use the **Limit** option under **Advanced Settings** to increase the number of entries in the view.

- 4 From the **Action** list box, select **Delete from Quarantine**.
- 5 Click **Start**.
- 6 In the dialog box that appears, click **Delete**.
- 7 In the confirmation dialog box that appears, click **OK**.

Managing the virus and spyware notifications that appear on client computers

You can decide whether or not notifications appear on client computers for virus and spyware events. You can customize messages about detections.

See [“Managing scans on client computers”](#) on page 405.

Table 17-20 Tasks for managing virus and spyware notifications that appear on client computers

Task	Description
Customize a scan detection message	<p>For Windows and Linux client computers, you can configure a detection message for the following types of scans:</p> <ul style="list-style-type: none"> ■ All types of Auto-Protect ■ Scheduled scans and on-demand scans <p>For scheduled scans, you can configure a separate message for each scan.</p> <p>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).</p> <p>For Mac client computers, you can configure a detection message that applies to all scheduled scans and a message that applies to on-demand scans.</p> <p>See “Customizing administrator-defined scans for clients that run on Windows computers” on page 469.</p> <p>See “Customizing administrator-defined scans for clients that run on Mac computers” on page 470.</p> <p>See “Customizing administrator-defined scans for clients that run on Linux computers” on page 472.</p>

Managing the virus and spyware notifications that appear on client computers**Table 17-20** Tasks for managing virus and spyware notifications that appear on client computers (*continued*)

Task	Description
Change settings for user notifications about Download Insight detections	<p>Applies to Windows client computers only.</p> <p>You can change the notifications that users receive about Download Insight detections.</p> <p>See “Managing Download Insight detections” on page 432.</p>
Change settings for user notifications about SONAR detections	<p>Applies to Windows client computers only.</p> <p>You can change the notifications that users receive about SONAR detections.</p> <p>See “Managing SONAR” on page 486.</p>
Choose whether or not to display the Auto-Protect results dialog	<p>Applies to Windows client computers only.</p> <p>Applies to Auto-Protect for the file system only.</p> <p>See “Customizing administrator-defined scans for clients that run on Windows computers” on page 469.</p>
Set up Auto-Protect email notifications	<p>Applies to Windows client computers only.</p> <p>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.</p> <p>For Internet Email Auto-Protect, you can also specify that a notification appears about scan progress when Auto-Protect scans an email.</p> <p>See “Customizing Auto-Protect for email scans on Windows computers” on page 468.</p>
Allow users to see scan progress and start or stop scans	<p>Applies to Windows client computers only.</p> <p>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.</p> <p>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.</p> <p>See “Allowing users to view scan progress and interact with scans on Windows computers” on page 480.</p>
Configure warnings, errors, and prompts	<p>Applies to Windows client computers only.</p> <p>You can enable or disable several types of alerts that appear on client computers about Virus and Spyware Protection events.</p> <p>See “Modifying miscellaneous settings for Virus and Spyware Protection on Windows computers” on page 475.</p>

Table 17-20 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	<p>Applies to clients that run on Windows 8.</p> <p>You can enable or disable the popup notifications that appear in the Windows 8 style user interface for detections and other critical events.</p> <p>See “Enabling or disabling Symantec Endpoint Protection pop-up notifications that appear on Windows 8 clients” on page 453.</p>

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 453.

See [“How Symantec Endpoint Protection handles detections on Windows 8 computers”](#) on page 422.

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 452.

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 and Windows Server 2012.

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 17-21 Managing ELAM detections

Task	Description
View the status of ELAM on your client computers	<p>You can see whether Symantec Endpoint Protection ELAM is enabled in the Computer Status log.</p> <p>See “Viewing logs” on page 613.</p>
View ELAM detections	<p>You can view early launch anti-malware detections in the Risk log.</p> <p>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.</p> <p>See “Viewing logs” on page 613.</p>
Enable or disable ELAM	<p>You might want to disable Symantec Endpoint Protection ELAM to help improve computer performance.</p> <p>See “Adjusting the Symantec Endpoint Protection early launch anti-malware (ELAM) options” on page 455.</p> <p>See “Adjusting scans to improve computer performance” on page 427.</p>

Table 17-21 Managing ELAM detections (*continued*)

Task	Description
Adjust ELAM detection settings if you get false positives	<p>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.</p> <p>Note: ELAM does not support a specific exception for an individual driver. The override option applies globally to ELAM detections.</p> <p>See “Adjusting the Symantec Endpoint Protection early launch anti-malware (ELAM) options” on page 455.</p>
Run Power Eraser on ELAM detections that Symantec Endpoint Protection cannot remediate	<p>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.</p> <p>See “Starting Power Eraser analysis from Symantec Endpoint Protection Manager” on page 770.</p> <p>See “Troubleshooting computer issues with the Symantec Help support tool” on page 744.</p>

Adjusting the Symantec Endpoint Protection early launch anti-malware (ELAM) options

Symantec Endpoint Protection provides an ELAM driver that works with the Microsoft ELAM driver to provide protection for the computers in your network when they start up. The settings are supported on Microsoft Windows 8 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 453.

See [“Troubleshooting computer issues with the Symantec Help support tool”](#) on page 744.

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 reputation data to make decisions about files”](#) on page 436.

See [“Configuring client groups to use private servers for reputation queries and submissions”](#) on page 457.

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 Advanced Threat Protection: Endpoint 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 Advanced Threat Protection: Endpoint**
This option redirects the reputation queries and submissions from clients in the group to ATP: Endpoint. ATP: Endpoint then sends the queries and submissions to Symantec. ATP: Endpoint servers gather data about client detections and provide forensic analysis. This option redirects antivirus, SONAR, and IPS submissions, but it does not redirect file reputation submissions. Symantec does not directly receive reputation queries or submissions from clients in the group.
- **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

Configuring client groups to use private servers for reputation queries and submissions

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. In that case, Symantec cannot receive any client submissions.

See [“Enabling or disabling client submissions to Symantec Security Response”](#) on page 442.

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.

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 for reputation queries and submissions

- 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.

Configuring client groups to use private servers for reputation queries and submissions

- 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**.

Customizing scans

This chapter includes the following topics:

- Customizing the virus and spyware scans that run on Windows computers
- Customizing the virus and spyware scans that run on Mac computers
- Customizing the virus and spyware scans that run on Linux computers
- Customizing Auto-Protect for Windows clients
- Customizing Auto-Protect for Mac clients
- Customizing Auto-Protect for Linux clients
- Customizing Auto-Protect for email scans on Windows computers
- Customizing administrator-defined scans for clients that run on Windows computers
- Customizing administrator-defined scans for clients that run on Mac computers
- Customizing administrator-defined scans for clients that run on Linux computers
- Randomizing scans to improve computer performance in virtualized environments on Windows clients
- Modifying global scan settings for Windows clients
- Modifying miscellaneous settings for Virus and Spyware Protection on Windows computers
- Modifying miscellaneous settings for Virus and Spyware Protection on Linux computers
- Customizing Download Insight settings

- [Changing the action that Symantec Endpoint Protection takes when it makes a detection](#)
- [Allowing users to view scan progress and interact with scans on Windows computers](#)
- [How Symantec Endpoint Protection interacts with Windows Security Center](#)

Customizing the virus and spyware scans that run on Windows computers

You can customize options for administrator-defined scans (scheduled and on-demand scans) that run on Windows computers. You can also customize options for Auto-Protect.

Table 18-1 Customizing virus and spyware scans on Windows computers

Task	Description
Customize Auto-Protect settings	<p>You can customize Auto-Protect in many ways, including the configuration for the following settings:</p> <ul style="list-style-type: none"> ■ 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 <p>You can also enable or disable the Scan Results dialog for Auto-Protect scans of the file system.</p> <p>See “Customizing Auto-Protect for Windows clients” on page 464.</p> <p>See “Customizing Auto-Protect for email scans on Windows computers” on page 468.</p>
Customize administrator-defined scans	<p>You can customize the following types of options for scheduled and on-demand scans.</p> <ul style="list-style-type: none"> ■ Compressed files ■ Tuning options ■ Insight Lookup ■ Advanced schedule options ■ User notifications about detections <p>See “Customizing administrator-defined scans for clients that run on Windows computers” on page 469.</p> <p>You can also customize scan actions.</p>

Table 18-1 Customizing virus and spyware scans on Windows computers
(continued)

Task	Description
Adjust ELAM settings	<p>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.</p> <p>See "Managing early launch anti-malware (ELAM) detections" on page 453.</p>
Adjust Download Insight settings	<p>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.</p> <p>See "Customizing Download Insight settings" on page 477.</p>
Customize scan actions	<p>You can change the action that Symantec Endpoint Protection takes when it makes a detection.</p> <p>See "Changing the action that Symantec Endpoint Protection takes when it makes a detection" on page 478.</p>
Customize global scan settings	<p>You might want to customize global scan settings to increase or decrease the protection on your client computers.</p> <p>See "Modifying global scan settings for Windows clients" on page 474.</p>
Customize miscellaneous options for Virus and Spyware Protection	<p>You can specify the types of risk events that clients send to Symantec Endpoint Protection Manager. You can also adjust how Symantec Endpoint Protection interacts with Windows Security Center.</p> <p>See "Modifying miscellaneous settings for Virus and Spyware Protection on Windows computers" on page 475.</p> <p>See "How Symantec Endpoint Protection interacts with Windows Security Center" on page 482.</p>

See ["Managing scans on client computers"](#) on page 405.

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 18-2 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 465.
Customize administrator-defined scans	You can customize common settings and notifications as well as scan priority. You can also enable or disable a warning to alert the user when definitions are out-of-date. See “Customizing administrator-defined scans for clients that run on Mac computers” on page 470.

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 18-3 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: <ul style="list-style-type: none"> ■ 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 <p>You can also enable or disable the Scan Results dialog for Auto-Protect scans of the file system.</p> <p>See “Customizing Auto-Protect for Linux clients” on page 466.</p>
Customize administrator-defined scans	You can customize the following types of options for scheduled and on-demand scans. <ul style="list-style-type: none"> ■ File and folder types ■ Compressed files ■ Security risks ■ Scheduling options ■ User notifications <p>You can also customize scan actions.</p>

Table 18-3 Customizing virus and spyware scans on Linux computers
(continued)

Task	Description
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 478.
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 miscellaneous settings for Virus and Spyware Protection on Linux computers” on page 476.

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, check or uncheck **Enable Auto-Protect**.

Note: If you disable Auto-Protect, Download Insight cannot function even if it is enabled.

- 4 Under **Scanning**, under **File types**, 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 478.

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 450.

- 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 461.

See [“Managing scans on client computers”](#) on page 405.

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 503.

- 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 462.
See [“Changing the action that Symantec Endpoint Protection takes when it makes a detection”](#) on page 478.
See [“Managing the virus and spyware notifications that appear on client computers”](#) on page 450.

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 478.

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 450.
- 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 463.

See [“Changing the action that Symantec Endpoint Protection takes when it makes a detection”](#) on page 478.

See [“Managing the virus and spyware notifications that appear on client computers”](#) on page 450.

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:
 - **Internet Email Auto-Protect**
 - **Microsoft Outlook Auto-Protect**
 - **Lotus Notes Auto-Protect**
- 3 On the **Scan Details** tab, check or uncheck **Enable Internet Email Auto-Protect**.
- 4 Under **Scanning**, under **File types**, 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 478.
- 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 461.

See [“Managing the virus and spyware notifications that appear on client computers”](#) on page 450.

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**.
- 5 On the **Compressed Files** tab, you can reduce the number of levels to scan compressed files. If you reduce the number of levels, you might improve client computer performance.
- 6 On the **Tuning** tab, change the tuning level for the best client computer performance or the best scan performance.
- 7 Click **OK**.

- 8 On the **Insight Lookup** tab, change any of the settings to adjust how Insight Lookup handles reputation detections. The settings are similar to the settings for Download Insight.
- 9 For scheduled scans only, on the **Schedule** tab, set any of the following options:
 - **Scan Duration**
You can set how long the scan runs before it pauses and waits until the client computer is idle. You can also randomize scan start time.
 - **Missed Scheduled Scans**
You can specify a retry interval for missed scans.
- 10 On the **Actions** tab, change any detection actions.
See [“Changing the action that Symantec Endpoint Protection takes when it makes a detection”](#) on page 478.
- 11 On the **Notifications** tab, enable or disable a notification that appears on client computers when the scan makes a detection.
See [“Managing the virus and spyware notifications that appear on client computers”](#) on page 450.
- 12 Click **OK**.
See [“Customizing the virus and spyware scans that run on Windows computers”](#) on page 461.
See [“Setting up scheduled scans that run on Windows computers”](#) on page 422.

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.
- 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 disable 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 462.

See [“Setting up scheduled scans that run on Mac computers”](#) on page 424.

See [“Changing the action that Symantec Endpoint Protection takes when it makes a detection”](#) on page 478.

See [“Managing the virus and spyware notifications that appear on client computers”](#) on page 450.

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 478.

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 450.

11 Click **OK**.

See [“Customizing the virus and spyware scans that run on Linux computers”](#) on page 463.

See [“Setting up scheduled scans that run on Linux computers”](#) on page 425.

See [“Changing the action that Symantec Endpoint Protection takes when it makes a detection”](#) on page 478.

See [“Managing the virus and spyware notifications that appear on client computers”](#) on page 450.

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 427.
- See [“Setting up scheduled scans that run on Windows computers”](#) on page 422.

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 405.

See [“Customizing the virus and spyware scans that run on Windows computers”](#) on page 461.

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 miscellaneous settings for Virus and Spyware Protection on Windows computers

Each Virus and Spyware Protection policy includes the options that apply to all virus and spyware scans that run on Windows client computers.

You can set the following options:

- Windows Security Center
 - You can specify how Windows Security Center works with Symantec Endpoint Protection.
- Internet Browser Protection
 - You can specify a default URL that Symantec Endpoint Protection uses when it repairs a security risk that changed a browser home page.
- Risk log events
 - By default, clients always send certain types of events to the management server (such as **Scan stopped** or **Scan started**). You can choose to send or not send other types of events (such as **File not scanned**).
 - The events that clients send to the management server affect information in reports and logs. You should decide what types of events that you want to forward to the management server. You can reduce the size of the logs and the amount of information that is included in reports if you select only certain types of events.
 - You can configure how long the client retains log items. The option does not affect any events that the clients send to the management console. You can use the option to reduce the actual log size on the client computers.
 - You can specify how often client computers send aggregated events to the management server.
- Miscellaneous notifications
 - Warn users when definitions are out-of-date or missing
 - You can display and customize warning messages to appear on client computers when their virus and security risk definitions are outdated or missing. You might want to alert users if you do not have automatic updates scheduled. In rare cases, users might see errors appear on their client computers during scans. For example, the client computer might encounter buffer overruns or decompression problems.
 - Include a URL in the error messages that appear during scans

Modifying miscellaneous settings for Virus and Spyware Protection on Linux computers

You can specify a URL that points to the Symantec support Web site or to a custom URL. For example, you might have an internal Web site that you want to specify instead.

Note: The URL also appears in the System event log for the client on which the error occurs.

- Virtual image exceptions

You can exclude virtual images from Auto-Protect or administrator-defined scans. You must create the baseline images that you want to exclude with the Virtual Image Exclusion tool.

To modify miscellaneous settings for Virus and Spyware Protection on Windows computers

- 1 In the console, open a Virus and Spyware Protection policy.
- 2 Under **Windows Settings**, click **Miscellaneous**.
Specify options for Windows Security Center or Internet Browser Protection.
- 3 On the **Log Handling** tab, set options for event filtering, log retention, and log aggregation.
- 4 On the **Notifications** tab, configure global notifications.
- 5 On the **Virtual Images** tab, configure virtual image exceptions.
- 6 Click **OK**.

See [“Customizing the virus and spyware scans that run on Windows computers”](#) on page 461.

See [“How Symantec Endpoint Protection interacts with Windows Security Center”](#) on page 482.

See [“Managing the virus and spyware notifications that appear on client computers”](#) on page 450.

Modifying miscellaneous settings for Virus and Spyware Protection on Linux computers

Each Virus and Spyware Protection policy includes the Miscellaneous options that apply to all virus and spyware scans that run on Linux client computers. These options apply entirely to log handling.

To modify miscellaneous settings for Virus and Spyware Protection on 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.

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 461.

See [“Managing Download Insight detections”](#) on page 432.

To customize Download Insight settings

- 1 In the console, open a Virus and Spyware Protection policy and select **Download Protection**.
- 2 On the **Download Insight** tab, make sure that **Enable Download Insight to detect potential risks in downloaded files based on file reputation** is checked.

If Auto-Protect is disabled, Download Insight cannot function even if it is enabled.

- 3 Move the slider for malicious file sensitivity to the appropriate level.

If you set the level higher, Download Insight detects more files as malicious and fewer files as unproven. Higher settings, however, return more false positives.

- 4 Check or uncheck the following options to use as additional criteria for examining unproven files:
 - **Files with fewer than x users**
 - **Files known by users for less than x days**

When unproven files meet this criteria, Download Insight detects the files as malicious.

Changing the action that Symantec Endpoint Protection takes when it makes a detection

- 5 Make sure that **Automatically trust any file downloaded from an intranet website** is checked.
- 6 On the **Actions** tab, under **Malicious Files**, specify a first action and a second action.
- 7 Under **Unproven Files**, specify the action.
- 8 On the **Notifications** tab, 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.

Changing the action that Symantec Endpoint Protection takes when it makes a detection

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 461.

See [“Customizing the virus and spyware scans that run on Mac computers”](#) on page 462.

See [“Customizing the virus and spyware scans that run on Linux computers”](#) on page 463.

See [“Managing Download Insight detections”](#) on page 432.

See [“Managing SONAR”](#) on page 486.

See [“Checking the scan action and rescanning the identified computers”](#) on page 404.

See [“Remediating risks on the computers in your network”](#) on page 401.

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.

Allowing users to view scan progress and interact with scans on Windows computers

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 405.

How Symantec Endpoint Protection interacts with Windows Security Center

Windows Security Center provides alerts on your client computers if any security software is out of date or if security settings should be strengthened. It is included with Windows XP Service Pack 2 or higher and Windows Vista. You can use a Virus and Spyware Protection policy to configure Windows Security Center settings on your client computers that run Windows XP Service Pack 3. As of Symantec Endpoint Protection 12.1.6, Windows Service Pack 2 is no longer supported. These settings do not apply to clients that run Windows Vista.

See [“Customizing administrator-defined scans for clients that run on Windows computers”](#) on page 469.

Note: The settings do not apply to Windows Action Center in Windows 7 and Windows 8.

Table 18-4 Options to configure how Windows Security Center works with the client

Option	Description	When to use
Disable Windows Security Center	<p>Lets you permanently or temporarily disable Windows Security Center on your client computers.</p> <p>Available options:</p> <ul style="list-style-type: none"> ■ 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. 	<p>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.</p> <p>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.</p>
Display antivirus alerts within Windows Security Center	<p>Lets you set antivirus alerts from the Symantec Endpoint Protection client to appear in the Windows notification area.</p>	<p>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.</p>
Display a Windows Security Center message when definitions are outdated	<p>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.</p>	<p>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).</p> <p>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.</p>

Managing SONAR

This chapter includes the following topics:

- [About SONAR](#)
- [Managing SONAR](#)
- [Handling and preventing SONAR false positive detections](#)
- [Adjusting SONAR settings on your client computers](#)
- [Monitoring SONAR detection results to check for false positives](#)

About SONAR

SONAR is a real-time protection that detects potentially malicious applications when they run on your computers. SONAR provides "zero-day" protection because it detects threats before traditional virus and spyware detection definitions have been created to address the threats.

SONAR uses heuristics as well as reputation data to detect emerging and unknown threats. SONAR provides an additional level of protection on your client computers and complements your existing Virus and Spyware Protection, intrusion prevention, and firewall protection.

SONAR uses a heuristics system that leverages Symantec's online intelligence network with proactive local monitoring on your client computers to detect emerging threats. SONAR also detects changes or behavior on your client computers that you should monitor.

Note: Auto-Protect also uses a type of heuristic that is called Bloodhound to detect suspicious behavior in files.

SONAR might inject some code into the applications that run in Windows user mode to monitor them for suspicious activity. In some cases, the injection might affect the application performance or cause problems with running the application. You can create an exception to exclude the file, folder, or application from this type of monitoring.

Note: SONAR does not inject code into applications on 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.

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.

See [“Managing SONAR”](#) on page 486.

See [“Managing exceptions in Symantec Endpoint Protection”](#) on page 495.

Managing SONAR

SONAR is part of Proactive Threat Protection on your client computers. You manage SONAR settings as part of a Virus and Spyware Protection policy. Many of the settings can be locked so that users on client computers cannot change the settings.

Table 19-1 Managing SONAR

Task	Description
Learn how SONAR works	<p>Learn how SONAR detects unknown threats. Information about how SONAR works can help you make decisions about using SONAR in your security network.</p> <p>See “About SONAR” on page 484.</p>
Check that SONAR is enabled	<p>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.</p> <p>You can use the Clients tab to check whether Proactive Threat Protection is enabled on your client computers.</p> <p>See “Adjusting SONAR settings on your client computers” on page 490.</p>
Check the default settings for SONAR	<p>SONAR settings are part of a Virus and Spyware Protection policy.</p> <p>See “About the default Virus and Spyware Protection policy scan settings” on page 417.</p>
Make sure that Insight lookups are enabled	<p>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.</p> <p>You enable or disable Insight Lookups in the Submissions dialog.</p> <p>See “Enabling or disabling client submissions to Symantec Security Response” on page 442.</p>

Table 19-1 Managing SONAR (continued)

Task	Description
<p>Monitor SONAR events to check for false positive detections</p>	<p>You can use the SONAR log to monitor events.</p> <p>You can also view the SONAR Detection Results report (under Risk Reports) to view information about detections.</p> <p>See “Monitoring SONAR detection results to check for false positives” on page 491.</p> <p>See “Monitoring endpoint protection” on page 593.</p>
<p>Adjust SONAR settings</p>	<p>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.</p> <p>You also might want to enable or disable notifications for high or low risk heuristic detections.</p> <p>See “Adjusting SONAR settings on your client computers” on page 490.</p> <p>See “Handling and preventing SONAR false positive detections” on page 488.</p>
<p>Prevent SONAR from detecting the applications that you know are safe</p>	<p>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.</p> <p>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.</p> <p>Note: If you set the action for high risk detections to log only, you might allow potential threats on your client computers.</p> <p>See “Handling and preventing SONAR false positive detections” on page 488.</p>

Table 19-1 Managing SONAR (continued)

Task	Description
Prevent SONAR from examining some applications	<p>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.</p> <p>See “Creating exceptions for Virus and Spyware scans” on page 498.</p>
Manage the way SONAR detects the applications that make DNS or host file changes	<p>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.</p> <p>See “Adjusting SONAR settings on your client computers” on page 490.</p> <p>See “Creating an exception for an application that makes a DNS or host file change” on page 510.</p>
Allow clients to submit information about SONAR detections to Symantec	<p>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.</p> <p>See “Enabling or disabling client submissions to Symantec Security Response” on page 442.</p>

Handling and preventing SONAR false positive detections

SONAR might make false positive detections for certain internal custom applications. Also, if you disable Insight lookups, the number of false positives from SONAR increases.

See [“Enabling or disabling client submissions to Symantec Security Response”](#) on page 442.

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 19-2 Handling SONAR false positives

Task	Description
Log SONAR high risk heuristic detections and use application learning	<p>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.</p> <p>See “Configuring the management server to collect information about the applications that the client computers run” on page 332.</p> <p>After the period of time, you should set the detection action back to Quarantine.</p> <p>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.</p> <p>See “Adjusting SONAR settings on your client computers” on page 490.</p>
Create exceptions for SONAR to allow safe applications	<p>You can create exceptions for SONAR in the following ways:</p> <ul style="list-style-type: none"> ■ Use the SONAR log to create an exception for an application that was detected and quarantined <p>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.</p> <p>See “Creating exceptions from log events in Symantec Endpoint Protection Manager” on page 511.</p> <p>See “Configuring how the Quarantine handles the rescanning of files after new definitions arrive” on page 448.</p> ■ Use an Exceptions policy to specify an exception for a particular file name, folder name, or application. <p>You can exclude an entire folder from SONAR detection. You might want to exclude the folders where your custom applications reside.</p> <p>See “Creating exceptions for Virus and Spyware scans” on page 498.</p>

Adjusting SONAR settings on your client computers

You might want to change the SONAR actions to reduce the rate of false positive detections. You might also want to change the SONAR actions to change the number of detection notifications that appear on your client computers.

Note: The settings for SONAR notifications are also used for TruScan proactive threat scan notifications.

To adjust SONAR settings on your client computers

- 1 In the Virus and Spyware Protection policy, select **SONAR**.
- 2 Make sure that **Enable SONAR** is checked.
- 3 Under **Scan Details**, change the actions for high or low risk heuristic threats.
You can enable aggressive mode for low risk detections. This setting increases SONAR sensitivity to low risk detections. It might increase the false positive detections.
- 4 Optionally change the settings for the notifications that appear on your client computers.
- 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 510.

6 Under **Suspicious Behavior Detection**, change the action for high or low risk detections.

7 Click **OK**.

See [“Managing SONAR”](#) on page 486.

See [“Creating exceptions for Virus and Spyware scans”](#) on page 498.

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: <ul style="list-style-type: none"> ■ A possible legitimate process is listed as a Potential risk found event. ■ A probable security risk is listed as a Security risk found event.
Application	The process name.
Application type	The type of malware that SONAR or a TruScan proactive threat scan detected.
File/Path	The path name from where the process was launched.

The **Event** column tells you immediately whether a detected process is a security risk or a possible legitimate process. However, a potential risk that is found may or may not be a legitimate process, and a security risk that is found may or may not be a malicious process. Therefore, you need to look at the **Application type** and **File/Path** columns for more information. For example, you might recognize the application name of a legitimate application that a third-party company has developed.

Legacy clients do not support SONAR. Legacy clients collect similar events from TruScan proactive threat scans, however, and include them in the SONAR log.

To monitor SONAR detection results to check for false positives

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

2 On the Logs tab, in the **Log type** drop-down list, click **SONAR**.

- 3 Select a time from the **Time range** list box closest to when you last changed a scan setting.
- 4 Click **Advanced Settings**.
- 5 In the **Event type** drop-down list, select one of the following log events:
 - To view all detected processes, make sure **All** is selected.
 - To view the processes that have been evaluated as security risks, click **Security risk found**.
 - To view the processes that have been evaluated and logged as potential risks, click **Potential risk found**.
- 6 Click **View Log**.
- 7 After you identify the legitimate applications and the security risks, create an exception for them in an Exceptions policy.

You can create the exception directly from the SONAR Logs pane.

See [“Creating exceptions from log events in Symantec Endpoint Protection Manager”](#) on page 511.

Managing Tamper Protection

This chapter includes the following topics:

- [About Tamper Protection](#)
- [Changing Tamper Protection settings](#)

About Tamper Protection

Tamper Protection provides real-time protection for Symantec applications that run on servers and clients. It prevents non-Symantec processes such as worms, Trojan horses, viruses, and security risks, from affecting Symantec resources. You can configure the software to block or log attempts to modify Symantec resources.

Note: Tamper Protection runs on Windows clients only. It does not run on Mac or Linux clients.

By default, Tamper Protection is enabled and is set to **Block and do not log**. You can change the setting to **Log only** or **Block and log** if you want to monitor the detections for false positives. Tamper Protection can generate many log messages, so you might not want to log the events.

If you use any third-party security risk scanners that detect and defend against unwanted adware and spyware, these scanners typically affect Symantec resources. If you set Tamper Protection to log tamper events when you run such a scanner, Tamper Protection generates a large number of log entries. If you decide to log Tamper Protection events, use log filtering to manage the number of events.

You can create exceptions for the applications that Tamper Protection detects.

See [“Changing Tamper Protection settings”](#) on page 494.

See [“Creating a Tamper Protection exception on Windows clients”](#) on page 509.

Changing Tamper Protection settings

Tamper Protection provides real-time protection for Symantec applications that run on servers and clients. It prevents threats and security risks from tampering with Symantec resources. You can enable or disable Tamper Protection. You can also configure the action that Tamper Protection takes when it detects a tampering attempt on the Symantec resources in your network.

Tamper Protection settings are configured globally for a selected group.

To change Tamper Protection settings

- 1 In the console, click **Clients**.
- 2 On the **Policies** tab, under **Settings**, click **General Settings**.
- 3 On the **Tamper Protection** tab, check or uncheck **Protect Symantec security software from being tampered with or shut down**.
- 4 In the list box under **Actions to take if an application attempts to tamper with or shut down Symantec security software**, select one of the following actions:
 - **Log only**
 - **Block and do not log**
 - **Block and log**
- 5 Click the icon to lock or unlock the options on client computers. When you lock an option, you prevent user changes to the option.
- 6 Click **OK**.

See [“About Tamper Protection”](#) on page 493.

Managing exceptions

This chapter includes the following topics:

- [Managing exceptions in Symantec Endpoint Protection](#)
- [About exceptions in Symantec Endpoint Protection to Virus and Spyware scans](#)
- [Creating exceptions for Virus and Spyware scans](#)
- [Restricting the types of exceptions that users can configure on client computers](#)
- [Creating exceptions from log events in Symantec Endpoint Protection Manager](#)

Managing exceptions in Symantec Endpoint Protection

You can manage exceptions for Symantec Endpoint Protection in the Symantec Endpoint Protection Manager console.

Table 21-1 Managing exceptions

Task	Description
Learn about exceptions	You use exceptions to exclude items from being scanned on your client computers. See “About exceptions in Symantec Endpoint Protection to Virus and Spyware scans” on page 497.

Table 21-1 Managing exceptions (*continued*)

Task	Description
Review the types of files and folders that Symantec Endpoint Protection automatically excludes from scans	<p>Symantec Endpoint Protection automatically creates exceptions, or exclusions, for some third-party applications and some Symantec products.</p> <p>You can also configure individual scans to scan only certain extensions and skip any other extensions.</p> <p>See “About the files and folders that Symantec Endpoint Protection excludes from virus and spyware scans” on page 414.</p>
Create exceptions for scans	<p>You add exceptions in an Exceptions policy directly. Or you can add exceptions from log events on the Monitors page.</p> <p>See “Creating exceptions for Virus and Spyware scans” on page 498.</p> <p>See “Creating exceptions from log events in Symantec Endpoint Protection Manager” on page 511.</p>
Restricting the types of exceptions that users can configure on client computers (Windows only)	<p>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.</p> <p>Users can never force an application detection and they never have permission to create Tamper Protection exceptions.</p> <p>Users also cannot create a file exception for application control.</p> <p>See “Restricting the types of exceptions that users can configure on client computers” on page 511.</p>

Table 21-1 Managing exceptions (*continued*)

Task	Description
Check the logs for detections for which you might want to create exceptions	<p>After Symantec Endpoint Protection makes a detection, you can create an exception for the detection from the log event.</p> <p>For example, you might want to create an exception for a file that scans detect but that your users request to download.</p> <p>See “Creating exceptions from log events in Symantec Endpoint Protection Manager” on page 511.</p>
Create exceptions for intrusion prevention signatures	<p>You can specify exceptions for intrusion prevention.</p> <p>You can also set up a list of excluded hosts for intrusion prevention.</p> <p>Intrusion prevention exceptions are configured in an Intrusion Prevention policy.</p> <p>See “Creating exceptions for IPS signatures” on page 387.</p>

About exceptions in Symantec Endpoint Protection to Virus and Spyware scans

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 21-2 Client type and scan exceptions

Client Type	Exception
Windows clients	<ul style="list-style-type: none"> ■ File ■ Folder ■ Known risk ■ Extension ■ Trusted Web domain ■ Application to monitor ■ Application ■ Tamper Protection
Mac clients	<ul style="list-style-type: none"> ■ File or folder exception
Linux clients	<ul style="list-style-type: none"> ■ Folder or extension exception

See “[About the files and folders that Symantec Endpoint Protection excludes from virus and spyware scans](#)” on page 414.

See “[Managing exceptions in Symantec Endpoint Protection](#)” on page 495.

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.

Note: The Exceptions policy includes a SONAR file path exception to prevent SONAR code injection into the specified application. SONAR does not inject code into applications on 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 or later clients. You can prevent SONAR code injection into applications on these clients, however, by creating an **Application to monitor** exception in the legacy policy. After the client learns the application, you can configure an application exception in the policy.

Exceptions for virus and spyware scans also apply to Download Insight.

Table 21-3 Creating exceptions for Symantec Endpoint Protection

Task	Description
Exclude a file from virus and spyware scans	<p>Supported on Windows and Mac clients.</p> <p>Excludes a file by name from virus and spyware scans, SONAR, or application control on Windows clients.</p> <p>See “Excluding a file or a folder from scans” on page 503.</p>
Exclude a folder from virus and spyware scans	<p>Supported on Windows, Mac, and Linux clients.</p> <p>Excludes a folder from virus and spyware scans, SONAR, or all scans on Windows clients.</p> <p>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.</p> <p>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.</p> <p>See “Excluding a file or a folder from scans” on page 503.</p>
Exclude a known risk from virus and spyware scans	<p>Supported on Windows clients.</p> <p>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.</p> <p>If a user configures custom actions for a known risk that you configure to ignore, Symantec Endpoint Protection ignores the custom actions.</p> <p>Security risk exceptions do not apply to SONAR.</p> <p>See “Excluding known risks from virus and spyware scans on Windows clients” on page 505.</p>

Table 21-3 Creating exceptions for Symantec Endpoint Protection (*continued*)

Task	Description
Exclude file extensions from virus and spyware scans	<p>Supported on Windows and Linux clients.</p> <p>Excludes any files with the specified extensions from virus and spyware scans.</p> <p>Extension exceptions do not apply to SONAR or to Power Eraser.</p> <p>See “Excluding file extensions from virus and spyware scans on Windows clients and Linux clients” on page 506.</p>
Monitor an application to create an exception for the application	<p>Supported on Windows clients.</p> <p>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.</p> <p>If you disable application learning, the Application to monitor exception forces application learning for the application that you specify.</p> <p>See “Monitoring an application to create an exception for the application on Windows clients” on page 507.</p>

Table 21-3 Creating exceptions for Symantec Endpoint Protection (*continued*)

Task	Description
Specify how virus and spyware scans handle monitored applications	<p>Supported on Windows clients.</p> <p>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.</p> <p>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.</p> <p>The application exception is a SHA-2 hash-based exception. Legacy exceptions for TruScan proactive threat scans appear as SHA-1 hash-based exceptions. Legacy 11.0 clients support SHA-1 exceptions only. The file fingerprint in the exceptions list is preceded by a 2 or a 1 respectively to indicate the file hash type.</p> <p>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.</p> <p>See "Specifying how Symantec Endpoint Protection handles monitored applications on Windows clients" on page 507.</p> <p>See "Configuring the management server to collect information about the applications that the client computers run" on page 332.</p>

Table 21-3 Creating exceptions for Symantec Endpoint Protection (*continued*)

Task	Description
Exclude a web domain from virus and spyware scans	<p>Supported on Windows clients.</p> <p>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.</p> <p>Download Insight must be enabled for the exception to have any effect.</p> <p>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.</p> <p>See the following related knowledge base articles:</p> <ul style="list-style-type: none"> ■ 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 <p>See “Excluding a trusted Web domain from scans on Windows clients” on page 508.</p>
Create file exceptions for Tamper Protection	<p>Supported on Windows clients.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>See “Creating a Tamper Protection exception on Windows clients” on page 509.</p>

Table 21-3 Creating exceptions for Symantec Endpoint Protection (*continued*)

Task	Description
Allow applications to make DNS or host file changes	<p>Supported on Windows clients</p> <p>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.</p> <p>See “Creating an exception for an application that makes a DNS or host file change” on page 510.</p>

See [“Managing exceptions in Symantec Endpoint Protection”](#) on page 495.

See [“Creating exceptions from log events in Symantec Endpoint Protection Manager”](#) on page 511.

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 498.

See [“Excluding file extensions from virus and spyware scans on Windows clients and Linux clients”](#) on page 506.

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 498.

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 498.

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 503.

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 498.

See [“Specifying how Symantec Endpoint Protection handles monitored applications on Windows clients”](#) on page 507.

See [“Creating exceptions from log events in Symantec Endpoint Protection Manager”](#) on page 511.

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.

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 507.

See [“Creating exceptions for Virus and Spyware scans”](#) on page 498.

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 510.

Excluding a trusted Web domain from scans on Windows clients

You can exclude a Web domain from virus and spyware scans and SONAR.

You must enter a single domain or IP address when you specify a trusted Web domain exception. You can specify only one domain at a time. Port numbers are not supported. You must specify an IP address for an FTP location.

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.

Note: If Download Insight or Auto-Protect is disabled, trusted Web domain exceptions are disabled as well.

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.

Note: You can specify a URL, but the exception uses only the domain name portion of a URL. If you specify a URL, you can pre-pend the URL with either HTTP or HTTPS (case-insensitive), but the exception applies to both. Regardless of whether a user navigates to the domain through HTTP or HTTPS, both Download Insight and SONAR exclude the domain. If the user navigates to any location within the domain, the user can download files from that location. You can specify an IP address, but it must be HTTP. For HTTPS, you can only specify a URL.

- 3 Click **OK**.
 - 4 Repeat the procedure to add more Web domain exceptions.
- See [“Creating exceptions for Virus and Spyware scans”](#) on page 498.

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 498.

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 498.

See [“Specifying how Symantec Endpoint Protection handles monitored applications on Windows clients”](#) on page 507.

See [“Adjusting SONAR settings on your client computers”](#) on page 490.

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 495.

Creating exceptions from log events in Symantec Endpoint Protection Manager

You can create exceptions from log events for virus and spyware scans, SONAR, application control, and Tamper Protection.

Note: You cannot create exceptions from log events for early launch anti-malware detections.

Table 21-4 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 in Symantec Endpoint Protection Manager

- 1 On the **Monitors** tab, click the **Logs** tab.
- 2 In the **Log type** drop-down list, select the Risk log, SONAR log, or Application and Device Control log.
- 3 If you selected Application and Device Control, select **Application Control** from the **Log content** list.
- 4 Click **View Log**.
- 5 Next to **Time range**, select the time interval to filter the log.
- 6 Select the entry or entries for which you want to create an exception.
- 7 Next to **Action**, select the type of exception that you want to create.

The exception type that you select must be valid for the item or items that you selected.
- 8 Click **Apply** or **Start**.
- 9 In the dialog box, remove any items that you do not want to include in the exception.

- 10 For security risks, check **Log when the security risk is detected** if you want Symantec Endpoint Protection to log the detection.
 - 11 Select all of the Exceptions policies that should use the exception.
 - 12 Click **OK**.
- See [“Monitoring endpoint protection”](#) on page 593.
- See [“Managing exceptions in Symantec Endpoint Protection”](#) on page 495.
- See [“Creating exceptions for Virus and Spyware scans”](#) on page 498.

Testing security policies

This chapter includes the following topics:

- [Testing Symantec Endpoint Protection Manager policies](#)
- [Testing a Virus and Spyware Protection policy](#)
- [Blocking a process from starting on client computers](#)
- [Preventing users from writing to the registry on client computers](#)
- [Preventing users from writing to a particular file](#)
- [Adding and testing a rule that blocks a DLL](#)
- [Adding and testing a rule that terminates a process](#)

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 22-1 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 515.

Table 22-1 Features that you can test (*continued*)

Feature	See this topic
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 516. See “Preventing users from writing to the registry on client computers” on page 517. See “Preventing users from writing to a particular file” on page 518. See “Adding and testing a rule that blocks a DLL ” on page 519. See “Adding and testing a rule that terminates a process” on page 520.

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://www.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 **Terminate process**, **Enable logging**, and **Notify user**.
- 13 Under **Notify user**, type **writing to terminate 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 Msvcr7.dll file contains the program code that is used to run various Windows applications such as Microsoft WordPad. If you add a rule that blocks Msvcr7.dll on the client computer, you cannot open Microsoft WordPad

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.

Enforcing policies and meeting compliance requirements

- [Chapter 23. Managing application control, device control, and system lockdown](#)
- [Chapter 24. Managing Host Integrity to enforce security policies](#)

Managing application control, device control, and system lockdown

This chapter includes the following topics:

- [About application and device control](#)
- [About Application and Device Control policies](#)
- [About the structure of an Application and Device Control policy](#)
- [Setting up application and device control](#)
- [Enabling a default application control rule set](#)
- [Creating custom application control rules](#)
- [Configuring system lockdown](#)
- [Managing device control](#)

About application and device control

You can use application and device control to monitor and control the behavior of applications on client computers and manage hardware devices that access client computers. You can also control applications by setting up system lockdown to allow only approved applications on client computers.

Note: Both application control and device control are supported on 32-bit and 64-bit computers.

You use an Application and Device Control policy to configure application control and device control on client computers. You use the **Policies** tab on the **Clients** page to set up system lockdown.

Warning: Application control and system lockdown are advanced security features that only experienced administrators should configure.

A summary of the application and device control features is given here.

Application control	<p>You can use application control to control applications in the following ways:</p> <ul style="list-style-type: none"> ■ Prevent malware from taking over applications ■ Restrict the applications that can run ■ Prevent users from changing configuration files ■ Protect specific registry keys ■ Protect particular folders, such as \WINDOWS\system
Device control	<p>You can use device control to control devices in the following ways:</p> <ul style="list-style-type: none"> ■ Block or allow different types of devices that attach to client computers, such as USB, infrared, and FireWire devices ■ Block or allow serial ports and parallel ports
System lockdown	<p>You can use system lockdown to control applications in the following ways:</p> <ul style="list-style-type: none"> ■ 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. <p>System lockdown ensures that your system stays in a known and trusted state.</p> <p>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.</p> <p>See “Configuring system lockdown” on page 541.</p>

See [“About Application and Device Control policies”](#) on page 525.

See [“Setting up application and device control”](#) on page 526.

About Application and Device Control policies

You can implement access control or device control on client computers by using an Application and Device Control policy. You can only assign one Application and Device Control policy at a time to a group or a location.

See [“About application and device control”](#) on page 523.

By default, there is an Application and Device Control policy on the management server. However, by default the Application and Device Control policy driver is disabled on the client. To enable the driver, you must either enable an existing rule or add and enable a new rule in the policy. After the policy applies to the client computer, a notification requests that the user restart the client computer. The user must restart the computer for the policy to take effect.

If you withdraw or disable the Application and Device Control policy, the driver is disabled and the client is not protected. When you enable the policy again, the user must restart the client computer again.

About the structure of an Application and Device Control policy

The application control portion of an Application and Device Control policy can contain multiple rule sets, and each rule set contains one or more rules. You can configure properties for a rule set, and properties, conditions, and actions for each rule.

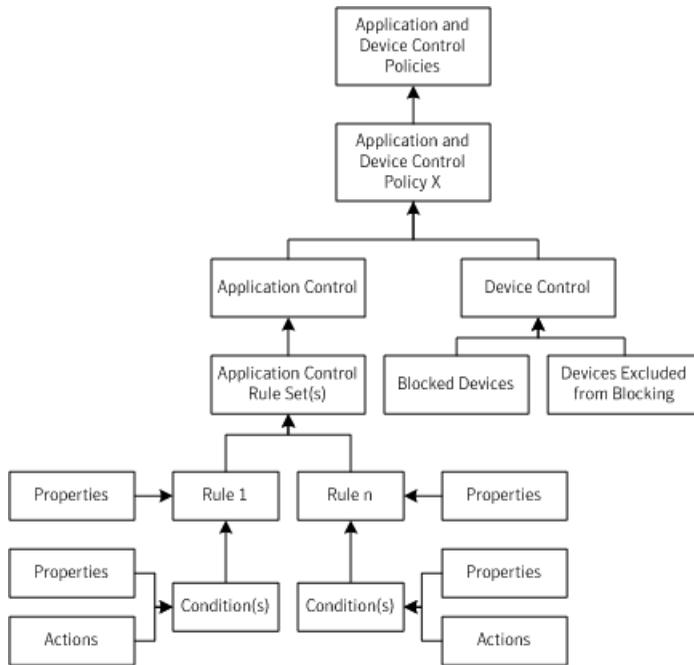
Rules control attempts to access computer entities, such as files or Windows registry keys, that Symantec Endpoint Protection monitors. You configure these different types of attempts as conditions. For each condition, you can configure actions to take when the condition is met. You configure rules to apply to only certain applications, and you can optionally configure them to exclude other applications from having the action applied.

See [“Creating custom application control rules”](#) on page 529.

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 23-1](#) illustrates the application and device control components and how they relate to each other.

Figure 23-1 Application and Device Control policy structure



Setting up application and device control

You can set up application and device control by performing some typical tasks.

See [“About application and device control”](#) on page 523.

Table 23-1 Setting up application and device control

Task	Description
<p>Enable default application control rule sets</p>	<p>Application and Device Control policies contain default application control rule sets. The default rule sets are disabled. You can enable any sets that you need.</p> <p>Note: If the default rule sets do not meet your requirements, create custom rule sets.</p> <p>The default rule sets are configured in production mode rather than test mode. However, you can change the setting to test mode and test the rules in your test network before you apply them to your production network.</p> <p>See “Enabling a default application control rule set” on page 528.</p> <p>Note: Client computers require a restart when you enable application control rules.</p> <p>See “Restarting the client computers from Symantec Endpoint Protection Manager” on page 129.</p>
<p>Create and test custom application control rule sets</p>	<p>You can create custom application control rule sets. Typically only advanced administrators should perform this task.</p> <p>See “Creating custom application control rules” on page 529.</p> <p>See “Typical application control rules” on page 533.</p> <p>Note: Client computers require a restart when you enable application control rules.</p>
<p>Create exceptions for application control</p>	<p>Application control might cause problems for some applications that you run in your network. You can exclude files or folders from application control. You use an Exceptions policy to specify the exception.</p> <p>Note: Symantec Endpoint Protection 12.1 included a separate application control exception. In the current release, an application control exception is created as part of the file or folder exceptions configuration.</p> <p>See “Excluding a file or a folder from scans” on page 503.</p>
<p>Set up system lockdown</p>	<p>System lockdown controls the applications on your client computers.</p> <p>See “Configuring system lockdown” on page 541.</p>
<p>Configure device control to allow or block hardware devices</p>	<p>Device control specifies what hardware devices are allowed or blocked on your client computers.</p> <p>Symantec Endpoint Protection Manager provides a device list that you can use in the device control configuration. You can add devices to the list.</p> <p>See “Managing device control” on page 565.</p>

Table 23-1 Setting up application and device control (*continued*)

Task	Description
View the Application Control and Device Control logs	<p>You can view the application control and device control events in the Application Control log and the Device Control log in Symantec Endpoint Protection Manager.</p> <p>On the client computer, application control and device control events appear in the Control log.</p> <p>Note: You might see duplicate or multiple log entries for a single application control action. For example, if explorer.exe tries to copy a file, it sets the write and delete bits of the file's access mask. Symantec Endpoint Protection logs the event. If the copy action fails because an application control rule blocks the action, explorer.exe tries to copy the file by using only the delete bit in the access mask. Symantec Endpoint Protection logs another event for the copy attempt.</p>
Prevent or allow users from enabling or disabling application and device control	<p>You can prevent or allow users from enabling or disabling application and device control on the client. Use the setting in the Client User Interface Settings dialog.</p> <p>See "Locking and unlocking settings by changing the user control level" on page 267.</p>

Enabling a default application control rule set

The application control portion of an Application and Device Control policy is made up of application control rule sets. Each application control rule set is made up of one or more rules. Default application control rule sets are installed with the Symantec Endpoint Protection Manager. The default rule sets are disabled at installation.

If you want to use the default rule sets in an Application and Device Control policy, you must enable them.

See ["Setting up application and device control"](#) on page 526.

To enable a default application control rule set

- 1 In the console, in the Application and Device Control policy to which you want to add a default application control rule set, click **Application Control**.
- 2 To review the setting in a default application control rule set, click the name under **Rule Set**, and then click **Edit**.

Be sure not to make any changes.

- 3 When you have finished reviewing the rules and their condition settings, click **Cancel**.
- 4 Check the check box next to each rule set that you want to enable.
 For example, next to the Block writing to USB drives rule set, check the check box in the Enabled column.
- 5 Click **OK**.

To test the rule set Block writing to USB drives

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

Creating custom application control rules

You might want to use custom application control rules when you set up application and device control.

See [“Setting up application and device control”](#) on page 526.

Table 23-2 Creating custom application control rules

Step	Action	Description
Step 1	Plan the rule set	<p>A new application rule set contains one or more administrator-defined rules. Each rule set and each rule has properties. Each rule can contain one or more conditions for monitoring applications and their access to specified files, folders, registry keys, and processes.</p> <p>You should review best practices before you create custom rules.</p> <p>See “Best practices for creating application control rules” on page 531.</p> <p>You can also review the structure of the default rule sets to see how they are constructed.</p>

Table 23-2 Creating custom application control rules (*continued*)

Step	Action	Description
Step 2	Create the rule set and add rules	<p>You can create multiple rules and add them to a single application control rule set. You can delete rules from the rules list and change their position in the rule set hierarchy as needed. You can also enable and disable rule sets or individual rules within a set.</p> <p>See “Creating a custom rule set and adding rules” on page 535.</p> <p>See “Typical application control rules” on page 533.</p> <p>You can copy and paste rule sets or individual rules within the same policy or between two policies. You might want to copy rules from the policies that you download from Symantec or from the test policies that contain rules that you want to use in production policies.</p> <p>See “Copying application rule sets or rules between Application and Device Control policies” on page 536.</p>
Step 3	Apply a rule to specific applications and exclude certain applications from the rule	<p>Every rule must have at least one application to which it applies. You can also exclude certain applications from the rule. You specify the applications on the Properties tab for the rule.</p> <p>See “Applying a rule to specific applications and excluding applications from a rule” on page 537.</p>

Table 23-2 Creating custom application control rules (*continued*)

Step	Action	Description
Step 4	Add conditions and actions to rules	<p>The condition specifies what the application tries to do when you want to control it.</p> <p>You can set any of the following conditions:</p> <ul style="list-style-type: none"> ■ Registry access attempts ■ File and folder access attempts ■ Launch process attempts ■ Terminate process attempts ■ Load DLL attempts <p>See “Adding conditions and actions to a custom application control rule” on page 539.</p> <p>You can configure any of the following actions to take on an application when it meets the configured condition:</p> <ul style="list-style-type: none"> ■ Continue processing other rules. ■ Allow the application to access the entity. ■ Block the application from accessing the entity. ■ Terminate the application that tries to access an entity. <p>Note: Remember that actions always apply to the process that is defined for the rule. They do not apply to a process that you define in a condition.</p>
Step 5	Test the rules	<p>You should test your rules before you apply them to your production network.</p> <p>Configuration errors in the rule sets that are used in an Application and Device Control policy can disable a computer or a server. The client computer can fail, or its communication with Symantec Endpoint Protection Manager can be blocked.</p> <p>See “Testing application control rule sets” on page 540.</p> <p>After you test the rules, you can apply them to your production network.</p>

Best practices for creating application control rules

You should plan your custom application control rules carefully.

See [“Creating custom application control rules”](#) on page 529.

See [“Typical application control rules”](#) on page 533.

When you create application control rules, keep in mind the following best practices:

Table 23-3 Best practices for application control rules

Best practice	Description	Example
Use one rule set per goal	A best practice is to create one rule set that includes all of the actions that allow, block, and monitor one given task.	<p>You want to block write attempts to all removable drives and you want to block applications from tampering with a particular application.</p> <p>To accomplish these goals, you should create two different rule sets. You should not create all of the necessary rules to accomplish both of these goals with one rule set.</p>
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 .	<p>You want to prevent all users from moving, copying, and creating files on USB drives.</p> <p>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.</p>
Use the Terminate process action sparingly	<p>The Terminate process action kills a process when the process meets the configured condition.</p> <p>Only advanced administrators should use the Terminate process action. Typically, you should use the Block access action instead.</p>	<p>You want to terminate Winword.exe any time that any process launches Winword.exe.</p> <p>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.</p> <p>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.</p>

Table 23-3 Best practices for application control rules (*continued*)

Best practice	Description	Example
Use the Terminate Process Attempts condition to protect processes	<p>The Terminate Process Attempts condition allows or blocks an application's ability to terminate a process on a client computer.</p> <p>The condition does not allow or prevent users from stopping an application by the usual methods, such as clicking Quit from the File menu.</p>	<p>Process Explorer is a tool that displays the DLL processes that have opened or loaded, and what resources the processes use.</p> <p>You might want to terminate Process Explorer when it tries to terminate a particular application.</p> <p>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.</p>

Typical application control rules

You might want to create custom application control rules to prevent users from opening applications, writing to files, or sharing files.

See [“Creating custom application control rules”](#) on page 529.

You can look at the default rule sets to help determine how to set up your rules. For example, you can edit the **Block applications from running** rule set to view how you might use a **Launch Process Attempts** condition.

See [“Enabling a default application control rule set”](#) on page 528.

Table 23-4 Typical application control rules

Rule	Description
Prevent users from opening an application	<p>You can block an application when it meets either of these conditions:</p> <ul style="list-style-type: none"> ■ 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 Msvcr7.dll on the client computer, users cannot open Microsoft WordPad. The rule also blocks any other application that uses the DLL.

Table 23-4 Typical application control rules (*continued*)

Rule	Description
Prevent users from writing to a particular file	<p>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.</p> <p>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.</p> <p>Use the File and Folder Access Attempts condition to create this type of rule.</p>
Block file shares on Windows computers	<p>You can create a custom rule that applies to all applications to disable local file and print sharing on Windows computers.</p> <p>Include the following conditions:</p> <ul style="list-style-type: none"> ■ 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). <p>You set the action for each condition to Block access.</p> <p>Note: After you apply the policy, you must restart client computers to completely disable file sharing.</p> <p>You can also use firewall rules to prevent or allow client computers to share files.</p> <p>See “Permitting clients to browse for files and printers in the network” on page 375.</p>

Table 23-4 Typical application control rules (*continued*)

Rule	Description
Prevent users from running peer-to-peer applications	<p>You can use application control to prevent users from running peer-to-peer applications on their computers.</p> <p>You can create a custom rule with a Launch Process Attempts condition. In the condition, you must specify all peer-to-peer applications that you want to block, such as LimeWire.exe or *.torrent. You can set the action for the condition to Block access or Terminate process.</p> <p>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.</p> <p>See “Managing intrusion prevention on client computers” on page 380.</p> <p>See “Creating a firewall policy” on page 339.</p>
Block write attempts to DVD drives	<p>Currently, Symantec Endpoint Protection Manager does not support a rule set that specifies the blocking of write attempts to DVD drives. You can select the option in the Application and Device Control policy, however, the option is not enforced. Instead, you can create an Application and Device Control policy that blocks specific applications that write to DVD drives.</p> <p>You should also create a Host Integrity policy that sets the Windows registry key to block write attempts to DVD drives.</p> <p>For the latest information, see the Symantec Knowledge Base document: How to block CD/DVD Writing in Windows 7</p>

Creating a custom rule set and adding rules

You can create multiple rules and add them to a single application control rule set. Create as many rules and as many rule sets as you need to implement the protection you want. You can delete rules from the rules list and change their position in the rule set hierarchy as needed. You can also enable and disable rule sets or individual rules within a set.

Note: If you create a custom rule that blocks access to a 32-bit-specific folder (such as Windows\system32), the rules does not work on 64-bit clients. You must also create a rule to block access to the Windows\syswow64 folder as well.

See [“Creating custom application control rules”](#) on page 529.

Creating a custom rule set and adding rules

- 1 In the console, open an Application and Device Control policy and click **Add**.
- 2 In the **Add Application Control Rule Set** dialog box, uncheck **Enable logging** if you do not want to log events about this rule set.
- 3 In the **Rule set name** text box, change the default name for the rule set.
- 4 In the **Description** field, type a description.
- 5 Change the default name for the rule in the **Rule name** text box, and then type a description of the rule.
- 6 Uncheck **Enable this rule** if you do not want to enable the rule at this time.
- 7 On the **Properties** tab, you specify the applications to which this rule applies and what applications should be excluded from the rule.

Each rule must have an application to which it applies.

See [“Applying a rule to specific applications and excluding applications from a rule”](#) on page 537.

Each rule must also have conditions and actions.

See [“Adding conditions and actions to a custom application control rule”](#) on page 539.

- 8 To add additional rules to the rule set, click **Add**, and then click **Add Rule**.
- 9 Click **OK**.

The new rule set appears and is configured for test mode. You should test new rule sets before you apply them to your client computers.

See [“Testing application control rule sets”](#) on page 540.

Copying application rule sets or rules between Application and Device Control policies

You can copy application control rule sets or individual rules between two different policies. You can also copy rule sets or rules within the same policy. The procedures here describe how to copy rule sets or rules between two different policies.

See [“Creating custom application control rules”](#) on page 529.

Copying application rule sets between Application and Device Control policies

- 1 In the console, open the Application and Device Control policy that contains the rule sets that you want to copy.
- 2 Click **Application Control**.

- 3 On the **Application Control** page, under **Application Control Rules Sets**, right-click the rule set that you want to copy, and then select **Copy**.
- 4 Click **OK** to close the current policy.
- 5 In the console, under **Application and Device Control Policies**, select the target policy.
 Under **Tasks**, click **Edit the policy**.
- 6 In the target policy, select **Application Control**.
- 7 Under **Application Control Rule Sets**, right-click and select **Paste**.

Copying application rules between Application and Device Control policies

- 1 In the console, open the Application and Device Control policy that contains the rule that you want to copy.
- 2 Click **Application Control**.
- 3 Select the rule set that you want to copy the rule from, and then click **Edit**.
- 4 Under **Rules**, right-click the rule that you want to copy and select **Copy**.
- 5 Click **OK** to close the rule set.
- 6 Click **OK** to close the policy.
- 7 In the console, under **Application and Device Control Policies**, select the target policy.
- 8 Under **Tasks**, click **Edit the policy**.
- 9 In the target policy, select **Application Control**.
- 10 Select the rule set to which you want to copy the rule, and then click **Edit**.
- 11 Under **Rules**, right-click and select **Paste**.

Applying a rule to specific applications and excluding applications from a rule

You can apply a rule to applications, and you can exclude applications from the rule's actions. You specify one list that contains the applications to which the rule applies (the inclusions). You specify another list that contains the applications to which the rule does not apply (the exclusions). To tie a rule to a specific application, you define that application in the Apply this rule to the following processes text field.

If you want to tie the rule to all applications except for a given set of applications, then you can use the following settings:

- In the Apply this rule to the following processes text box, define a wildcard character for all processes (*).

- In the Do not apply this rule to the following processes text box, list the applications that need an exception.

You can define as many applications as you want for each list.

Note: Every rule must have at least one application listed in the **Apply this rule to the following processes** text box.

When you add applications to a rule, you can use the following ways to specify the application:

- The process name
- Wildcard characters
- Regular expressions
- File fingerprints
- The drive types from where the application was launched
- The device ID

See [“Creating custom application control rules”](#) on page 529.

To apply a rule to specific applications and to exclude a rule

- 1 In the **Edit Application Control Rule Set** dialog box, click the rule that you want to apply.
- 2 If you want to configure an application to apply the rule to, then to the right of Apply this rule to the following processes, click **Add**.
- 3 In the **Add Process Definition** dialog box, configure the following items:
 - Type the name of the application that you want to match in this rule.
 - Click either **Use wildcard matching (* and ? supported)** or **Use regular expression matching** for matching the name.
 - If desired, check the specific drive types on which to match the process.
 - If desired, check **Only match processes running on the following device id type**, and then type a device ID type in the text field or click **Select** to select a device ID type from the list in the Device Selection dialog box to only match the processes that run on devices of that ID type.
 - If desired, click **Options** to match processes based on the file fingerprint and to match only the processes that have a designated argument. You can choose to match the arguments exactly or by using regular expression matching.

- 4 Click **OK**.
 You can repeat steps 2 through 4 to add as many applications as you want.
- 5 If you want to configure one or more applications to exclude from the rule, then to the right of the **Do not apply this rule to the following processes** text field, click **Add**.
 Repeat the configuration of the applications to exclude as desired. You have the same options when you define an application to exclude as you have when you apply the rule to an application.
- 6 When you have finished defining the applications, click **OK**.

Adding conditions and actions to a custom application control rule

After you define what applications a custom rule applies to, you should define the conditions and actions for a rule. A condition's properties specify what the condition looks for. Its actions define what happens when the condition is met.

See ["Creating custom application control rules"](#) on page 529.

Adding conditions and actions to an application control rule

- 1 In the **Add Application Control Rule Set** or **Edit Application Control Rule Set** dialog box, under **Rules**, click **Add**, and then click **Add Condition**.
- 2 Select one of the following conditions:
 - **Registry Access Attempts**
 - **File and Folder Access Attempts**
 - **Launch Process Attempts**
 - **Terminate Process Attempts**
 - **Load DLL Attempts**
- 3 On the **Properties** tab for the condition, type a name and a description for the condition.
- 4 To the right of **Apply to the following entity**, where *entity* represents registry keys, files and folders, processes, or DLLs, click **Add**.

- 5 In the **Add entity Definition** dialog box, type the registry key, file or folder name, process name, or DLL.

Note: When you apply a condition to all entities in a particular folder, a best practice is to use *folder_name** or *folder_name***. One asterisk includes all the files and folders in the named folder. Use *folder_name*** to include every file and folder in the named folder plus every file and folder in every subfolder.

- 6 Click **OK**.
- 7 To the right of the **Do not apply to the following processes**, click **Add**, and specify the registry keys, files and folders, processes, or DLLs.
- 8 Click **OK**.
- 9 On the **Actions** tab for the condition, select one of the following actions:

- **Continue processing other rules**
- **Allow access**
- **Block access**
- **Terminate process**

For the **Registry Access Attempts** and **File and Folder Access Attempts** conditions, you can configure two sets of actions, one for **Read Attempt** and one for **Create, Delete or Write Attempt**.

- 10 Check **Enable logging**, and then select a severity level to assign to the entries that are logged.
- 11 Check **Notify user**, and then type the text that you want to user to see.
- 12 Click **OK**.

Testing application control rule sets

After you create custom application control rules, you should test them in your network.

See [“Creating custom application control rules”](#) on page 529.

Table 23-5 Testing application control rule sets

Step	Description
<p>Configure the rule set for test mode and enable or disable rules</p>	<p>You test rule sets by setting the mode to Test (log only) mode. Test mode creates a log entry to indicate when rules in the rule set would be applied without actually applying the rule.</p> <p>Custom rules use Test mode by default. You can also test default rules sets.</p> <p>You might want to test rules within the set individually. You can test individual rules by enabling or disabling them in the rule set.</p> <p>See “Creating a custom rule set and adding rules” on page 535.</p> <p>See “Enabling a default application control rule set” on page 528.</p>
<p>Apply the Application and Device Control policy to computers in your test network</p>	<p>If you created a new Application and Device Control policy, you need to apply the policy to clients in your test network.</p> <p>See “Assigning a policy to a group” on page 323.</p> <p>Note: Client computers must restart after you apply a new Application and Device Control policy or when you change the default policy.</p>
<p>Check the Control log</p>	<p>After you run your rule sets in Test mode for a period of time, you can check the client’s logs for any errors.</p> <p>You can view the Application Control log in Symantec Endpoint Protection Manager.</p> <p>You can also view the Control log on the client computer.</p> <p>When the rules function like you expect them to, you can change the rule set mode to Production mode.</p>

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 23-6 System lockdown steps

Step	Action	Description
Step 1	Create file fingerprint lists	<p>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.</p> <p>Note: 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.</p> <p>You can create a file fingerprint list in the following ways:</p> <ul style="list-style-type: none"> ■ 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 548. ■ Create a file fingerprint list with any third-party checksum utility. ■ In 12.1.6, you can run the Collect File Fingerprint List command from the console on a single computer or small group of computers. 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 261. <p>Note: In 12.1.6, if you run ATP: Endpoint in your network, you might see file fingerprint lists from ATP: Endpoint.</p> <p>See “Interaction between system lockdown and ATP: Endpoint blacklist rules” on page 552.</p>

Table 23-6 System lockdown steps (*continued*)

Step	Action	Description
Step 2	Import file fingerprint lists into Symantec Endpoint Protection Manager	<p>Before you can use a file fingerprint list in the system lockdown configuration, the list must be available in Symantec Endpoint Protection Manager.</p> <p>When you create file fingerprint lists with a checksum tool, you must manually import the lists into Symantec Endpoint Protection Manager.</p> <p>See “Importing or merging file fingerprint lists in Symantec Endpoint Protection Manager” on page 550.</p> <p>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.</p> <p>You can also export existing file fingerprint lists from Symantec Endpoint Protection Manager.</p>
Step 3	Create application name lists for approved or unapproved applications	<p>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.</p> <p>You can also manually enter individual application names in the system lockdown configuration.</p> <p>Note: A large number of named applications might affect client computer performance when system lockdown is enabled in blacklist mode.</p> <p>See “Creating an application name list to import into the system lockdown configuration” on page 553.</p>

Table 23-6 System lockdown steps (*continued*)

Step	Action	Description
Step 4	Set up and test the system lockdown configuration	<p>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.</p> <p>To set up and run the test, complete the following steps:</p> <ul style="list-style-type: none"> ■ 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. <p>See “Setting up and testing the system lockdown configuration before you enable system lockdown” on page 559.</p>
Step 5	View the unapproved applications and modify the system lockdown configuration if necessary	<p>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.</p> <p>The logged events also appear in the Application Control log.</p> <p>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.</p> <p>See “Setting up and testing the system lockdown configuration before you enable system lockdown” on page 559.</p>

Table 23-6 System lockdown steps (*continued*)

Step	Action	Description
Step 6	Enable system lockdown	<p>By default, system lockdown runs in whitelist mode. You can configure system lockdown to run in blacklist mode instead.</p> <p>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.</p> <p>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.</p> <p>See “Running system lockdown in whitelist mode” on page 561.</p> <p>See “Running system lockdown in blacklist mode” on page 562.</p>

Table 23-6 System lockdown steps (*continued*)

Step	Action	Description
Step 7	Update file fingerprint lists for system lockdown	<p>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:</p> <ul style="list-style-type: none"> ■ 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 551. See “Importing or merging file fingerprint lists in Symantec Endpoint Protection Manager” on page 550. ■ 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 554. See “Creating an application name list to import into the system lockdown configuration” on page 553. ■ 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. <p>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.</p> <p>See “Setting up and testing the system lockdown configuration before you enable system lockdown” on page 559.</p>

Table 23-6 System lockdown steps (*continued*)

Step	Action	Description
Step 8	Test selected items before you add or remove them when system lockdown is enabled	<p>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.</p> <p>You might want to remove file fingerprint lists if you have many lists and no longer use some of them.</p> <p>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.</p> <ul style="list-style-type: none"> ■ 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. <p>See “Testing selected items before you add or remove them when system lockdown is already enabled” on page 564.</p>

See [“Setting up application and device control”](#) on page 526.

Creating a file fingerprint list with checksum.exe

You can use the checksum.exe utility to create a file fingerprint list. The list contains the path and the file name and corresponding checksum for each executable file or DLL that resides in a specified path on the computer. The utility is installed with Symantec Endpoint Protection on the client computer.

You can also use a third-party utility to create a file fingerprint list.

You import the file fingerprint list into Symantec Endpoint Protection Manager to use in your system lockdown configuration.

See [“Configuring system lockdown”](#) on page 541.

The format of each line is *checksum_of_the_file* space *full_pathname_of_the_exe_or_DLL*.

An example of checksum.exe output is shown here:

```
0bb018fad1b244b6020a40d7c4eb58b7 c:\dell\openmanage\remind.exe
35162d98c2b445199fef95e838feae4b c:\dell\pnp\m\co\HSFCI008.dll
4f3ef8d2183f927300ac864d63dd1532 c:\dell\pnp\m\co\HXFSetup.exe
dcd15d648779f59808b50f1a9cc3698d c:\dell\pnp\m\co\MdmXSdk.dll
2f276c59243d3c051547888727d8cc78 c:\Nokia Video Manager\QtCore4.dll
e6b635b6f204b9f2a43ba7df8780a7a6 c:\Nokia Video Manager\QtNetwork4.dll
0901d37ec3339ef06dba0a9afb0ac97c c:\Nokia Video Manager\QtXml4.dll
a09eaad7f8c7c4df058bbaffd938cd4c c:\Nokia Video Manager\VideoManager.exe
```

To create a file fingerprint list with checksum.exe

- 1 Open a command prompt window on the computer that contains the image for which you want to create a file fingerprint list.

The computer must have Symantec Endpoint Protection client software installed.

- 2 Navigate to the folder that contains the file checksum.exe. Typically, the file is located in the following folder:

```
C:\Program Files\Symantec\Symantec Endpoint Protection\<version number>\bin
```

- 3 Type the following command:

```
checksum.exe outputfile path
```

where *outputfile* is the name of the text file that contains the checksums for all the applications that are located on the specified drive. The output file is a text file (*outputfile.txt*).

The following is an example of the syntax you could use to create a fingerprint list for an image:

```
checksum.exe cdrive.txt c:
```

This command creates a file that is called cdrive.txt. It contains the checksums and file paths of all the executables and DLLs found on the C drive of the client computer on which it was run.

The following is an example of the syntax that you could use to create a fingerprint for a folder on the client computer:

```
checksum.exe blocklist.txt c:\Files
```

This command creates a file that is called blocklist.txt. It contains the checksums and file paths of any executables and DLLs found in the Files folder.

Importing or merging file fingerprint lists in Symantec Endpoint Protection Manager

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 541.

See [“Creating a file fingerprint list with checksum.exe”](#) on page 548.

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 ATP: Endpoint sends to Symantec Endpoint Protection Manager.

See [“Importing or merging file fingerprint lists in Symantec Endpoint Protection Manager”](#) on page 550.

See [“Configuring system lockdown”](#) on page 541.

To update a file fingerprint list in Symantec Endpoint Protection Manager

- 1 In the console, click **Policies**.
- 2 Under **Policies**, expand **Policy Components**, and then click **File Fingerprint Lists**.
- 3 In the **File Fingerprint Lists** pane, select the fingerprint list that you want to edit.
- 4 Click **Edit**.
- 5 In the **Edit File Fingerprint Wizard**, click **Next**.
- 6 Do one of the following:
 - Click **Append a fingerprint file to this file fingerprint** to add a new file to an existing one.

- Click **Append another file fingerprint to this file fingerprint** to merge file fingerprint lists that you already imported.
 - Click **Replace an existing list with a new file fingerprint list**.
 - Click **Remove fingerprints from an existing list that match fingerprints in a new list**.
- 7 Do one of the following:
- Click **Browse** to locate the file or type the full path of the file fingerprint list that you want to append, replace, or remove.
 - Select the file fingerprints that you want to merge.
- 8 Click **Next**.
- 9 Click **Close**.
- 10 Click **Finish**.

Interaction between system lockdown and ATP: Endpoint blacklist rules

If your network includes ATP: Endpoint, you might see blacklists in the system lockdown configuration from ATP: Endpoint.

ATP: Endpoint blacklists interact with the system lockdown configuration in the following ways:

- When Symantec Endpoint Protection Manager receives a blacklist rule from ATP: Endpoint, 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 ATP: Endpoint.
- 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 ATP: Endpoint blacklist rule.
- If you disable system lockdown and delete the ATP: Endpoint blacklist, Symantec Endpoint Protection Manager automatically re-enables system lockdown and applies the blacklist.
- If you disable system lockdown but do not delete the ATP: Endpoint blacklist, system lockdown remains disabled until you re-enable it.

Note: ATP: Endpoint sends whitelist rules directly to Symantec Endpoint Protection clients. ATP: Endpoint does not send whitelist file fingerprints to Symantec Endpoint Protection Manager.

See [“Running system lockdown in whitelist mode”](#) on page 561.

See [“Running system lockdown in blacklist mode”](#) on page 562.

See [“Configuring client groups to use private servers for reputation queries and submissions”](#) on page 457.

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 1 or 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 23-7 Example matching mode settings

Application Name	Test Before Addition or Test Before Removal	Matching Mode
aa.exe	Disabled	Wildcard
bb.exe	Disabled	Regular expression
cc.exe	Enabled	Wildcard
dd.exe	Enabled	Wildcard
c:\program files\ee.exe	Disabled	Wildcard

See [“Configuring system lockdown”](#) on page 541.

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 23-8 Updating whitelists or blacklists for system lockdown

Step	Task	Description
Step 1	Create updated file fingerprint lists or application name lists and compress the files	<p>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.</p> <p>See “Creating a file fingerprint list with checksum.exe” on page 548.</p> <p>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.</p> <p>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.</p>
Step 2	Create an index.ini file	<p>The index.ini file specifies which file fingerprint lists and application names lists Symantec Endpoint Protection Manager should update.</p> <p>You can create an index.ini file with any text editor and copy the file to the specified URL.</p> <p>See “Creating an index.ini file for automatic updates of whitelists and blacklists that are used for system lockdown” on page 556.</p>
Step 3	Make the compressed file and index.ini available to Symantec Endpoint Protection Manager	<p>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.</p> <p>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: <code>..\Symantec Endpoint Protection Manager\data\inbox\WhitelistBlacklist\content</code>. 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.</p>

Table 23-8 Updating whitelists or blacklists for system lockdown (*continued*)

Step	Task	Description
Step 4	Enable automatic whitelist and blacklist updates in the management console	<p>You must enable the automatic update of existing whitelists or blacklists in the Symantec Endpoint Protection Manager console.</p> <p>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.</p> <p>See “Enabling automatic updates of whitelists and blacklists for system lockdown” on page 557.</p>
Step 5	Check the status of automatic updates for the whitelist or blacklist	<p>You can make sure that Symantec Endpoint Protection Manager completes the updates by checking the status in the console.</p> <p>See “Checking the status of automatic whitelist or blacklist updates for system lockdown” on page 558.</p>

See [“Manually updating a file fingerprint list in Symantec Endpoint Protection Manager”](#) on page 551.

See [“Configuring system lockdown”](#) on page 541.

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 554.

See [“Creating an application name list to import into the system lockdown configuration”](#) on page 553.

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 554.

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 554.

See [“Viewing logs”](#) on page 613.

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 be available in Symantec Endpoint Protection Manager.

See [“Importing or merging file fingerprint lists in Symantec Endpoint Protection Manager”](#) on page 550.

- 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 553.

- 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 541.
See [“Setting up firewall rules”](#) on page 367.

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 559.

Note: If you run system lockdown enabled in whitelist mode, Symantec Endpoint Protection Manager does not apply any blacklist rules from ATP: Endpoint.

See [“Interaction between system lockdown and ATP: Endpoint blacklist rules”](#) on page 552.

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 541.

See [“Disabling and enabling a group's inheritance”](#) on page 247.

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 ATP: Endpoint in your network, the ATP: Endpoint configuration affects the system lockdown blacklist configuration.

See [“Interaction between system lockdown and ATP: Endpoint blacklist rules”](#) on page 552.

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 559.

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 and enabling a group's inheritance”](#) on page 247.
- 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 559.

See [“Configuring system lockdown”](#) on page 541.

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 561.

See [“Running system lockdown in blacklist mode”](#) on page 562.

- 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 559.

See [“Configuring system lockdown”](#) on page 541.

Managing device control

You use the hardware devices list and an Application and Device Control policy to manage device control.

See [“Setting up application and device control”](#) on page 526.

See [“About application and device control”](#) on page 523.

See [“About Application and Device Control policies”](#) on page 525.

Table 23-9 Managing device control

Action	Description
Review the default hardware devices list in Symantec Endpoint Protection Manager	By default, Symantec Endpoint Protection Manager includes a list of hardware devices. The list appears on the Policies tab in Symantec Endpoint Protection Manager under Policy Components . You use this list to select the devices that you want to control on your client computers. If you want to control a device that is not included in the list, you must add the device first. See “About the hardware devices list” on page 566.
Add devices to the hardware devices list (if necessary)	When you add a device to the device list, you need a class ID or device ID for the device. See “Adding a hardware device to the Hardware Devices list” on page 568. See “Obtaining a class ID or device ID” on page 567.
Configure device control	Specify the devices that you want to block or exclude from blocking. See “Configuring device control” on page 569.

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 565.

You can add devices to the list. You cannot edit or delete any default devices.

Devices are identified by a device ID or class ID. You use either of these values to add a device to the list.

See [“Obtaining a class ID or device ID”](#) on page 567.

class ID	<p>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:</p> <pre>{00000000-0000-0000-0000-000000000000}</pre>
device ID	<p>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.</p> <p>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.</p> <p>The following is a device ID for a specific USB SanDisk device:</p> <pre>USBSTOR\DISK&VEN_SANDISK&PROD_CRUZER_MICRO&REV_2033\0002071406&0</pre> <p>The following is a device ID with a wildcard that indicates any USB SanDisk device:</p> <pre>USBSTOR\DISK&VEN_SANDISK*</pre> <p>The following is a device ID with a wildcard that indicates any USB disk device:</p> <pre>USBSTOR\DISK*</pre> <p>The following is a device ID with a wildcard that indicates any USB storage device:</p> <pre>USBSTOR*</pre>

Obtaining a class ID or device ID

You can use the Symantec DevViewer tool to obtain either the class ID (GUID) or the device ID. You can use Windows Device Manager to obtain the device ID.

After you obtain a device ID, you can modify it with a wildcard character to indicate a less specific group of devices.

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

- 1 In the installation file, locate the `\Tools\DevViewer` folder, and then download the `DevViewer.exe` tool to the client computer.
- 2 On the client computer, run `DevViewer.exe`.

- 3 Expand the Device Tree and locate the device for which you want the device ID or the GUID.
 For example, expand DVD-ROM drives and select the device within that category.
- 4 In the right-hand pane, right-click the device ID (which begins with [device ID]), and then click **Copy Device ID**.
- 5 Click **Exit**.
- 6 On the management server, paste the device ID into the list of hardware devices.

To obtain a device ID from Control Panel

- 1 Open the Device Manager from the Control Panel.
 The path to the Device Manager depends on the Windows operating system. For example, in Windows 7, click **Start > Control Panel > System > Device Manager**.
- 2 In the **Device Manager** dialog box, right-click the device, and click **Properties**.
- 3 In the device's **Properties** dialog box, on the **Details** tab, select the Device ID.
 By default, the Device ID is the first value displayed.
- 4 Copy the ID string.
- 5 Click **OK**.
 See [“Adding a hardware device to the Hardware Devices list”](#) on page 568.

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 566.

To add hardware devices to the Hardware Devices list

- 1 In the console, click **Policies**.
- 2 Under **Policies**, expand **Policy Components** and click **Hardware Devices**.
- 3 Under **Tasks**, click **Add a Hardware Device**.
- 4 Enter the name of the device you want to add.
 Both Class IDs and Device IDs are enclosed in curly braces by convention.

- 5 Select either **Class ID** or **Device ID**, and paste the ID that you copied from the Windows Device Manager or the DevViewer tool.
- 6 You can use wildcard characters to define a set of device IDs. For example, you can use the following string: `*IDE\DVDROM*`.
 See [“Obtaining a class ID or device ID”](#) on page 567.
- 7 Click **OK**.

Configuring device control

You use an Application and Device Control policy to configure device control. You have already added any devices you need to the Hardware Devices list.

See [“Managing device control”](#) on page 565.

See [“About application and device control”](#) on page 523.

Configuring device control

- 1 In the console, open an Application and Device Control policy.
- 2 Click **Device Control**.
- 3 Under **Blocked Devices**, click **Add**.
- 4 In the **Device Selection** window, select one or more devices. Make sure that if you block 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 **Specify Message Text** to type the message that appears in the notification.
- 10 Click **OK**.

Managing Host Integrity to enforce security policies

This chapter includes the following topics:

- [How Host Integrity works](#)
- [Setting up Host Integrity](#)
- [About Host Integrity requirements](#)
- [Adding predefined requirements to a Host Integrity policy](#)
- [Setting up remediation for a predefined Host Integrity requirement](#)
- [Configuring the frequency of Host Integrity check settings](#)
- [Allowing the Host Integrity check to pass if a requirement fails](#)
- [Configuring notifications for Host Integrity checks](#)
- [Creating a Quarantine policy for a failed Host Integrity check](#)
- [Configuring peer-to-peer authentication for Host Integrity enforcement](#)
- [Adding a custom requirement from a template](#)
- [Writing a customized requirement script](#)
- [Creating a test Host Integrity policy with a custom requirement script](#)

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 24-1](#) describes the process to enforce security compliance on the client computer.

Table 24-1 Process for Host Integrity

Step	Action	Description
Step 1	The client computer runs a Host Integrity check on the client computer.	<p>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.</p> <p>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.</p> <p>See “Setting up Host Integrity” on page 572.</p>
Step 2	The Host Integrity check passes or fails	<ul style="list-style-type: none"> ■ 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. <p>See “Allowing the Host Integrity check to pass if a requirement fails” on page 579.</p> <p>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.</p> <p>See “Configuring peer-to-peer authentication for Host Integrity enforcement” on page 582.</p>

Table 24-1 Process for Host Integrity (*continued*)

Step	Action	Description
Step 3	Non-compliant computers remediate a failed Host Integrity check (optional)	<ul style="list-style-type: none"> ■ 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 576. ■ 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 581. ■ 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	<p>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.</p> <ul style="list-style-type: none"> ■ 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. <p>You can view the results of the Host Integrity check in the Compliance log. See “Viewing logs” on page 613.</p>

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 24-2](#) lists the steps you need to perform to set up security compliance using Host Integrity policies.

Table 24-2 Tasks to set up Host Integrity policies

Step	Action	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	<p>When you add a new policy, perform the following tasks:</p> <ol style="list-style-type: none"> 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 574. See “Adding predefined requirements to a Host Integrity policy” on page 575. 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 576. 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	<ul style="list-style-type: none"> ■ Configure how often the Host Integrity check runs. See “Configuring the frequency of Host Integrity check settings” on page 579. ■ Configure whether or not users can cancel remediation. See “Allowing users to delay or cancel Host Integrity remediation” on page 577. ■ 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 580.
Step 3 (optional)	Set up peer-to-peer enforcement	<p>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.</p> <p>See “Configuring peer-to-peer authentication for Host Integrity enforcement” on page 582.</p>

Table 24-2 Tasks to set up Host Integrity policies (*continued*)

Step	Action	Description
Step 4 (optional)	Set up a Quarantine policy for non-compliant and unremediated computers	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 581.

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 24-3](#) lists the types of requirements you can use.

Table 24-3 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, antispymware 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 575.

Table 24-3 Requirement types for Host Integrity policies (*continued*)

Type	Description
<p>Custom requirements from templates</p>	<p>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.</p> <p>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.</p> <p>See “Adding a custom requirement from a template” on page 583.</p> <p>See “Configuring a site to download content updates” on page 189.</p>
<p>Custom requirements</p>	<p>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.</p> <p>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.</p> <p>See “Writing a customized requirement script” on page 584.</p>

See [“Setting up Host Integrity”](#) on page 572.

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 either the **Windows** or **Mac** client platform.

- 4 In the **Select requirement** drop-down list, select a predefined requirement, and then click **OK**.
- 5 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 576.

For more information, click **Help**.

- 6 Click **OK**.
- 7 Assign the policy to groups or locations.
- 8 Click **OK**.

See [“Adding a custom requirement from a template”](#) on page 583.

See [“Writing a customized requirement script”](#) on page 584.

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 572.

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 575.
- 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 577.
- 7 Click **OK**. See [“Allowing the Host Integrity check to pass if a requirement fails”](#) on page 579.

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 575.
- 2 In the **Add Requirement** dialog box, set up remediation.
 See [“Setting up remediation for a predefined Host Integrity requirement”](#) on page 576.
- 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 575.

See [“Allowing the Host Integrity check to pass if a requirement fails”](#) on page 579.

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 575.
See [“Writing a customized requirement script”](#) on page 584.
- 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 577.

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 576.

See [“About Host Integrity requirements”](#) on page 574.

Configuring peer-to-peer authentication for Host Integrity enforcement

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 Threat Protection Traffic log.

Note: Peer-to-peer authentication works in server control and mixed control, but not in client control.

To configure peer-to-peer authentication for Host Integrity enforcement

- 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 339.
- See [“Setting up Host Integrity”](#) on page 572.
- See [“Locking and unlocking settings by changing the user control level”](#) on page 267.

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 either the **Windows** or **Mac** client platform.
- 4 In the **Select requirement** drop-down list, click **Use existing templates**, and then click **OK**.

- 5 In the **Host Integrity Online Updating** dialog box, expand **Templates**, and then select a template category.
- 6 Next to each template you want to add, click **Add**.
- 7 Click **Import**.
- 8 Click **OK**.

See [“About Host Integrity requirements”](#) on page 574.

See [“Configuring a site to download content updates”](#) on page 189.

See [“Configuring the types of content used to update client computers”](#) on page 196.

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 either the **Windows** or **Mac** client platform.
- 4 In the **Select requirement** drop-down list, select **Custom requirement**, and then click **OK**.
- 5 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.

- 6 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**.

- 7 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.
- 8 Under the **Select a condition** drop-down list, specify the additional information that is required.
- 9 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.
- 10 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.
- 11 In the right-hand pane, define the criteria that you added.
 For more information on these options, click **Help**.
- 12 To add more nested statements, conditions, or functions, under **Customized Requirement Script**, right-click the node, and then click **Add**.
- 13 Repeat steps 10 to 12 as needed.

14 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**.

15 Click **OK**.

See [“Creating a test Host Integrity policy with a custom requirement script”](#) on page 589.

See [“Adding predefined requirements to a Host Integrity policy”](#) on page 575.

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 either the **Windows** or **Mac** client platform.
- 4 In the **Select requirement** drop-down list, select **Custom requirement**, and then click **OK**.

See [“Writing a customized requirement script”](#) on page 584.

- 5 In the **Custom Requirement** dialog box, under **Customized Requirement Script**, select the node where you want to add the function.
- 6 Click **Add**, and then click **Function**.
- 7 Click **Utility: Run a script**.
- 8 Enter a file name for the script, such as **myscript.js**.
- 9 Type the content of the script.
- 10 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.

- 11 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.

- 12 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.

- 13 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 either the **Windows** or **Mac** client platform.
- 4 In the **Select requirement** drop-down list, select **Custom requirement**, and then click **OK**.

See [“Writing a customized requirement script”](#) on page 584.

- 5 In the **Custom Requirement** dialog box, under **Customized Requirement Script**, select the node where you want to add the function.
- 6 Click **Add**, and then click **Function**.
- 7 Click **Utility: Set Timestamp**.
- 8 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 584.
- 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 584.
- 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 590.
- Test the Host Integrity policy you have created.
 See [“To test the Host Integrity policy on the client computer”](#) on page 591.

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 either **Windows** or **Mac**.
- 4 In the **Select requirement** drop-down list, click **Custom requirement**, and then click **OK**.
- 5 In the **Name** box, type a name for the custom requirement.
- 6 In the **Custom Requirement** dialog box, under **Customized Requirement Script**, right-click **Insert statements below**, and then click **Add > IF..THEN**.
- 7 In the right pane, in the **Select a condition** drop-down list, click **Utility: Operating System is**.
- 8 Under **Operating system**, check one or more operating systems that your client computers run and that you can test.
- 9 Under **Customized Requirement Script**, right-click **THEN //Insert statements here**, and then click **Add > Function > Utility: Show message dialog**.
- 10 In the **Caption of the message box** field, type a name to appear in the message title.
- 11 In the **Text of the message box** field, type the text that you want the message to display.
- 12 In the left pane, under **Customized Requirement Script**, click **Pass**.
- 13 In the right pane, under **As the result of the requirement, return**, check **Fail**, and then click **OK**.
- 14 Click **OK**.

- 15 In the **Host Integrity Policies** dialog box, in the left panel, click **Assign the policy**.
- 16 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 584.

See [“Writing a custom requirement to increment a registry DWORD value”](#) on page 589.

See [“Writing a custom requirement to run a script on the client”](#) on page 587.

Monitoring and reporting

- [Chapter 25. Monitoring protection with reports and logs](#)
- [Chapter 26. Managing notifications](#)

Monitoring protection with reports and logs

This chapter includes the following topics:

- [Monitoring endpoint protection](#)
- [Configuring reporting preferences](#)
- [Logging on to reporting from a stand-alone Web browser](#)
- [About the types of reports](#)
- [Running and customizing quick reports](#)
- [Saving and deleting custom reports](#)
- [How to generate scheduled reports](#)
- [Editing the filter used for a scheduled report](#)
- [Printing and saving a copy of a report](#)
- [Viewing logs](#)

Monitoring endpoint protection

Symantec Endpoint Protection collects information about the security events in your network. You can use log and reports to view these events, and you can use notifications to stay informed about the events as they occur.

You can use the reports and logs to determine the answers to the following kinds of questions:

- Which computers are infected?

- Which computers need scanning?
- What risks were detected in the network?

Note: Symantec Endpoint Protection pulls the events that appear in the reports from the event logs on your management servers. The event logs contain time-stamps in the client computers' time zones. When the management server receives the events, it converts the event time-stamps to Greenwich Mean Time (GMT) for insertion into the database. When you create reports, the reporting software displays information about events in the local time of the computer on which you view the reports.

Table 25-1 Tasks for monitoring endpoint protection

Task	Description
Review the security status of your network	<p>The following list describes some of the tasks that you can perform to monitor the security status of your client computers.</p> <ul style="list-style-type: none"> ■ View the number of clients that did not get installed. See “Running a report on the deployment status of clients” on page 600. ■ View the number of computers that are offline. See “Finding offline computers” on page 598. ■ Obtain a count of detected viruses and other security risks and view details for each virus and security risk. See “Viewing risks” on page 599. ■ Obtain a count of unprotected computers in your network and view the details for each computer. See “Viewing system protection” on page 597. ■ View the number of computers with up-to-date virus and spyware definitions. See “Viewing system protection” on page 597. ■ View the real-time operational status of your client computers. See “Viewing the protection status of clients and client computers” on page 253. ■ Review the processes that run in your network. See “Monitoring SONAR detection results to check for false positives” on page 491. ■ Locate which computers are assigned to which groups. ■ View a list of the Symantec Endpoint Protection software versions that are installed on the clients and Symantec Endpoint Protection Manager servers in your network. See “Generating a list of the Symantec Endpoint Protection versions installed on the clients and servers in your network” on page 602. ■ 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 101. <p>See “Viewing a daily or weekly status report” on page 597.</p>

Table 25-1 Tasks for monitoring endpoint protection (*continued*)

Task	Description
Locate which client computers need protection	<p>You can perform the following tasks to view or find which computers need additional protection:</p> <ul style="list-style-type: none">■ View the number of computers with Symantec Endpoint Protection disabled. See “Viewing system protection” on page 597.■ View the number of computers with out-of-date virus and spyware definitions. See “Viewing system protection” on page 597.■ Find the computers that have not been scanned recently. See “Finding unscanned computers” on page 598.■ View attack targets and sources. See “Viewing attack targets and sources” on page 601.■ View event logs. See “Viewing logs” on page 613.
Protect your client computers	<p>You can run commands from the console to protect the client computers.</p> <p>See “Running commands on client computers from the console” on page 261.</p> <p>For example, you can eliminate security risks on client computers.</p> <p>See “Checking the scan action and rescanning the identified computers” on page 404.</p>
Configure notifications to alert you when security events occur	<p>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.</p> <p>See “Setting up administrator notifications” on page 630.</p>
Create custom quick reports and scheduled reports for ongoing monitoring	<p>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.</p> <p>See “Running and customizing quick reports” on page 606.</p> <p>See “How to generate scheduled reports” on page 609.</p> <p>See “Saving and deleting custom reports” on page 608.</p> <p>See “Configuring reporting preferences” on page 602.</p>

Table 25-1 Tasks for monitoring endpoint protection (*continued*)

Task	Description
Minimize the amount of space that client logs take	<p>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.</p> <p>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.</p> <p>You can reduce the volume of log data by performing the following tasks:</p> <ul style="list-style-type: none"> ■ 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 708. ■ Specify how many log entries the client computer can keep in the database, and how long to keep them. See “Specifying how long to keep log entries in the database” on page 709. ■ Filter the less important risk events and system events out so that less data is forwarded to the server. See “Modifying miscellaneous settings for Virus and Spyware Protection on Windows computers” on page 475. ■ Reduce the number of clients that each management server manages. ■ Reduce the heartbeat frequency, which controls how often the client logs are uploaded to the server. See “Configuring push mode or pull mode to update client policies and content” on page 170. ■ 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 709.
Export log data to a centralized location	<p>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.</p> <p>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.</p> <p>See “Exporting log data to a text file” on page 706.</p> <p>See “Exporting data to a Syslog server” on page 705.</p> <p>See “Exporting log data to a comma-delimited text file” on page 707.</p> <p>See “Viewing logs from other sites” on page 618.</p>

Table 25-1 Tasks for monitoring endpoint protection (*continued*)

Task	Description
Troubleshoot issues with reports and logs	You can troubleshoot some issues with reporting. See “Troubleshooting reporting issues” on page 758.

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 593.

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 593.

To view system protection

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

Finding offline computers

You can list the computers that are offline.

A client may be offline for a number of reasons. You can identify the computers that are offline and remediate these problems in a number of ways.

See [“Troubleshooting communication problems between the management server and the client”](#) on page 745.

To find offline computers

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

To view offline client computers in the Computer Status log

- 1 In the console, click **Monitors**.
- 2 On the **Logs** tab, from the **Log type** list box, click **Computer Status**.
- 3 Click **Advanced Settings**.
- 4 In the Online status list box, click **Offline**.
- 5 Click **View Log**.

By default, a list of the computers that have been offline for the past 24 hours appears. The list includes each computer's name, IP address, and the last time that it checked in with its server. You can adjust the time range to display offline computers for any time range you want to see.

Finding unscanned computers

You can list the computers that need scanning.

See [“Monitoring endpoint protection”](#) on page 593.

To find unscanned computers

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

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

- 3 Click **Create Report**.

Viewing risks

You can get information about the risks in your network.

See [“Monitoring endpoint protection”](#) on page 593.

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**.

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 593.

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 attack targets and sources

You can view attack targets and sources.

See [“Monitoring endpoint protection”](#) on page 593.

To view the top targets that were attacked

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

Report type You select **Network Threat Protection**.

Select a report You select **Top Targets Attacked**.

- 3 Click **Create Report**.

To view top attack sources

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

Report type You select **Network Threat Protection**.

Select a report You select **Top Sources of Attack**.

- 3 Click **Create Report**.

A full report contains the following statistics:

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

To view a full report on attack targets and sources

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

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

- 3 Click **Create Report**.

Generating a list of the Symantec Endpoint Protection versions installed on the clients and servers in your network

You can run a quick report from Symantec Endpoint Protection Manager that provides a list of the Symantec Endpoint Protection software versions that are installed on the clients and Symantec Endpoint Protection Manager servers in your network. This list can be useful when you want to upgrade or migrate your software from a previous version of Symantec Endpoint Protection. The list includes local and remote computers.

You can save the report using MHTML Web page archive format.

See [“Printing and saving a copy of a report”](#) on page 612.

To generate a report that lists the Symantec Endpoint Protection software versions

- 1 In the console, click **Reports**.
- 2 For **Report type**, select **Computer Status**.
- 3 For **Select a report**, select **Symantec Endpoint Protection Product Versions**.
- 4 Click **Create Report**.

Configuring reporting preferences

You can configure the following reporting preferences:

- The **Home** and **Monitors** pages display options
- The **Security Status** thresholds
- The display options that are used for the logs and the reports, as well as legacy log file uploading

The security status thresholds that you set determine when the Security Status message on the Symantec Endpoint Protection Manager **Home** page is considered Poor. Thresholds are expressed as a percentage and reflect when your network is considered to be out of compliance with your security policies.

For example, you can set the percentage of computers with out-of-date virus definitions that triggers a poor security status. You can also set how many days old the definitions need to be to qualify as out of date. Symantec Endpoint Protection determines what is current when it calculates whether signatures or definitions are out of date as follows. Its standard is the most current virus definitions and IPS signature dates that are available on the management server on which the console runs.

For information about the preference options that you can set, you can click **Help** on each tab in the **Preferences** dialog box.

To configure reporting preferences

- 1 In the console, on the **Home** page, click **Preferences**.
- 2 Click one of the following tabs, depending on the type of preferences that you want to set:
 - **Home and Monitors**
 - **Security Status**
 - **Logs and Reports**
- 3 Set the values for the options that you want to change.
- 4 Click **OK**.

Logging on to reporting from a stand-alone Web browser

You can access the **Home**, **Monitors**, and **Reports** pages from a stand-alone Web browser that is connected to your management server. However, all of the other console functions are not available when you use a stand-alone browser.

Report pages and log pages always display in the language that the management server was installed with. To display these pages when you use a remote console or browser, you must have the appropriate font installed on the computer that you use.

To access reporting from a Web browser, you must have the following information:

- The host name of the management server.

Note: When you type the HTTPS standalone reporting URL in your browser, the browser might display a warning. The warning appears because the certificate that the management server uses is self-signed. To work around this issue, you can install the certificate in your browser's trusted certificate store. The certificate supports host names only, so use the host name in the URL. If you use localhost, IP address, or the fully qualified domain name, a warning still appears.

- Your user name and password for the management server.

Note: You must have Internet Explorer 6.0 or later installed. Other Web browsers are not supported.

To log on to reporting from a stand-alone Web browser

- 1 Open a Web browser.
- 2 Type the default reporting URL into the address text box in the following format:

https://management server host name:8445/reporting

Note: The Symantec Endpoint Protection version 11 default reporting URL is **http://management server address:8014/reporting**. If you migrate from version 11, you must update your browser's bookmarks.

- 3 When the logon dialog box appears, type your user name and password, and then click **Log On**.

If you have more than one domain, in the **Domain** text box, type your domain name.

About the types of reports

The following categories of reports are available:

- Quick reports, which you run on demand.
- Scheduled reports, which run automatically based on a schedule that you configure.

Reports include the event data that is collected from your management servers as well as from the client computers that communicate with those servers. You can customize reports to provide the information that you want to see.

The quick reports are predefined, but you can customize them and save the filters that you used to create the customized reports. You can use the custom filters to create custom scheduled reports. When you schedule a report to run, you can configure it to be emailed to one or more recipients.

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 25-2](#) describes the types of reports that are available.

Table 25-2 Report types available as quick reports and scheduled reports

Report type	Description
Audit	Displays the information about the policies that clients and locations use currently. It includes information about policy modification activities, such as the event times and types, policy modifications, domains, sites, administrators, and descriptions.
Application and Device Control	Displays the information about events where some type of behavior was blocked. These reports include information about application security alerts, blocked targets, and blocked devices. Blocked targets can be Windows registry keys, DLLs, files, and processes.
Compliance	Displays the information about the how many client 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.
Network Threat Protection	Displays the information about intrusion prevention, attacks on the firewall, and about firewall traffic and packets. The Network Threat Protection reports let you track a computer's activity and its interaction with other computers and networks. They record information about the traffic that tries to enter or exit the computers through their network connections.

Table 25-2 Report types available as quick reports and scheduled reports
(continued)

Report type	Description
Risk	Displays the information about risk events on your management servers and their clients. It includes information about SONAR scans and, if you have 11.0 clients in your network, about TruScan proactive threat scans.
Scan	Displays the information about virus and spyware scan activity.
System	Displays the information about event times, event types, sites, domains, servers, and severity levels. The System reports contain information that is useful for troubleshooting client problems.

If you have multiple domains in your network, many reports let you view data for all domains, one site, or a few sites. The default for all quick reports is to show all domains, groups, servers, and so on, as appropriate for the report you select to create.

See [“Running and customizing quick reports”](#) on page 606.

See [“How to generate scheduled reports”](#) on page 609.

Running and customizing quick reports

Quick reports are predefined, customizable reports. These reports include event data collected from your management servers as well as the client computers that communicate with those servers. Quick reports provide information on events specific to the settings you configure for the report. You can save the report settings so that you can run the same report at a later date, and you can print and save reports.

Quick reports are static; they provide information specific to the time frame you specify for the report. Alternately, you can monitor events in real time using the logs.

To run a quick report

- 1 In the console, click **Reports**.
- 2 On the **Quick Reports** tab, in the **Report type** list box, select the type of report that you want to run.

- 3 In the **Select a report** list box, select the name of the report you want to run.
- 4 Click **Create Report**.

To customize a quick report

- 1 In the console, click **Reports**.
- 2 On the **Quick Reports** tab, in the **Report type** list box, select the type of report that you want to customize.
- 3 In the **Select a report** list box, select the name of the report you want to customize.

For the **Network Compliance Status** report and the **Compliance Status** report, in the **Status** list box, select a saved filter configuration that you want to use, or leave the default filter.

For the **Top Risk Detections Correlation** report, you can select values for the **X-axis** and **Y-axis** list boxes to specify how you want to view the report.

For the **Scan Statistics Histogram Scan** report, you can select values for **Bin width** and **Number of bins**.

For some reports, you can specify how to group the report results in the **Group** list box. For other reports, you can select a target in the **Target** field on which to filter report results.

- 4 In the **Use a saved filter** list box, select a saved filter configuration that you want to use, or leave the default filter.
- 5 Under **What filter settings would you like to use?**, in the **Time range** list box, select the time range for the report.
- 6 If you select **Set specific dates**, then use the **Start date** and **End date** list boxes. These options set the time interval that you want to view information about.

When you generate a Computer Status report and select **Set specific dates**, you specify that you want to see all entries that involve a computer that has not checked in with its server since the time you specify in the date and time fields.

- 7 If you want to configure additional settings for the report, click **Advanced Settings** and set the options that you want.

You can click **Tell me more** to see descriptions of the filter options in the context-sensitive help.

Note: The filter option text boxes that accept wildcard characters and search for matches are not case-sensitive. The ASCII asterisk character is the only asterisk character that can be used as a wildcard character.

You can save the report configuration settings if you think you will want to run this report again in the future.

- 8 Click **Create Report**.

See [“Saving and deleting custom reports”](#) on page 608.

See [“Printing and saving a copy of a report”](#) on page 612.

See [“How to generate scheduled reports”](#) on page 609.

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 611.

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 account roles and access rights”](#) on page 293.

To save a custom report

- 1 In the console, click **Reports**.
- 2 On the **Quick Reports** tab, select a report type from the list box.
- 3 Change any basic settings or advanced settings for the report.
- 4 Click **Save Filter**.
- 5 In the **Filter name** text box, type a descriptive name for this report filter. Only the first 32 characters of the name that you give display when the filter is added to the **Use a saved filter** list.
- 6 Click **OK**.
- 7 When the confirmation dialog box appears, click **OK**.

After you save a filter, it appears in the **Use a saved filter** list box for related reports and logs.

To delete a custom report

- 1 In the console, click **Reports**.
- 2 On the **Quick Reports** tab, select a report type.
- 3 In the **Use saved filter** list box, select the name of the filter that you want to delete.
- 4 Click the **Delete** icon beside the **Use a saved filter** list box.
- 5 When the confirmation dialog box appears, click **Yes**.

How to generate 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 708.

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 generate 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** to save the scheduled report configuration.

Editing the filter used for a scheduled report

You can change the settings for any report that you have already scheduled. The next time the report runs it uses the new filter settings. You can also create additional scheduled reports, which you can base on a previously saved report filter.

Filter storage is based in part on the creator, so problems do not occur when two different users create a filter with the same name. However, an individual user or two users who log on to the default admin account should not create filters with the same name.

If users create filters with the same name, a conflict can occur under two conditions:

- Two users are logged on to the default admin account on different sites and each creates a filter with the same name.
- One user creates a filter, logs on to a different site, and immediately creates a filter with the same name.

If either condition occurs before site replication takes place, the user subsequently sees two filters with the same name in the filter list. Only one of the filters is usable. If this problem occurs, it is a best practice to delete the usable filter and recreate it with a different name. When you delete the usable filter, you also delete the unusable filter.

See [“Saving and deleting custom reports”](#) on page 608.

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 generate scheduled reports”](#) on page 609.

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 606.

To print a copy of a report

- 1 In the report window, click **Print**.
- 2 In the **Print** dialog box, select the printer you want, if necessary, and then click **Print**.

When you save a report, you save a snapshot of your security environment that is based on the current data in your reporting database. If you run the same report later, based on the same filter configuration, the new report shows different data.

To save a copy of a report

- 1 In the report window, click **Save**.
- 2 In the **File Download** dialog box, click **Save**.
- 3 In the **Save As** dialog box, in the **Save in selection** dialog box, browse to the location where you want to save the file.
- 4 In the **File name** list box, change the default file name, if desired.

5 Click **Save**.

The report is saved in MHTML Web page archive format in the location you selected.

6 In the **Download complete** dialog box, click **Close**.

Viewing logs

You can generate a list of events to view from your logs that are based on a collection of filter settings that you select. Each log type and content type have a default filter configuration that you can use as-is or modify. You can also create and save new filter configurations. These new filters can be based on the default filter or on an existing filter that you created previously. If you save the filter configuration, you can generate the same log view at a later date without having to configure the settings each time. You can delete your customized filter configurations if you no longer need them.

Note: If database errors occur when you view the logs that include a large amount of data, you might want to change the database timeout parameters.

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

See [“Changing timeout parameters for reviewing reports and logs”](#) on page 759.

Because logs contain some information that is collected at intervals, you can refresh your log views. To configure the log refresh rate, display the log and select from the **Auto-Refresh** list box at the top right on that log's view.

Note: If you view log data by using specific dates, the data stays the same when you click **Auto-Refresh**.

Reports and logs always display in the language that the management server was installed with. To display these when you use a remote Symantec Endpoint Protection Manager console or browser, you must have the appropriate font installed on the computer that you use.

See [“What you can do from the logs”](#) on page 614.

See [“Saving and deleting custom logs by using filters”](#) on page 617.

To view a log

- 1 In the main window, click **Monitors**.
- 2 On the **Logs** tab, from the **Log type** list box, select the type of log that you want to view.
- 3 For some types of logs, a **Log content** list box appears. If it appears, select the log content that you want to view.
- 4 In the **Use a saved filter** list box, select a saved filter or leave the value **Default**.
- 5 Select a time from the **Time range** list box or leave the default value. If you select **Set specific dates**, then set the date or dates and time from which you want to display entries.
- 6 Click **Advanced Settings** to limit the number of entries you display.

You can also set any other available **Advanced Settings** for the type of log that you selected.

Note: The filter option fields that accept wildcard characters and search for matches are not case-sensitive. The ASCII asterisk character is the only asterisk character that can be used as a wildcard character.

- 7 After you have the view configuration that you want, click **View Log**.

The log view appears in the same window.

What you can do from the logs

Logs contain records about client configuration changes, security-related activities, and errors. These records are called events. The logs display these events with any relevant additional information. Security-related activities include information about virus detections, computer status, and the traffic that enters or exits the client computer.

Logs are an important method for tracking each client computer's activity and its interaction with other computers and networks. You can use this data to analyze the overall security status of the network and modify the protection on the client computers. You can track the trends that relate to viruses, security risks, and attacks. If several people use the same computer, you might be able to identify who introduces risks, and help that person to use better precautions.

You can view the log data on the **Logs** tab of the **Monitors** page.

The management server regularly uploads the information in the logs from the clients to the management server. You can view this information in the logs or in

reports. Because reports are static and do not include as much detail as the logs, you might prefer to monitor the network by using logs.

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 261.
- Add several kinds of exceptions.
See [“Creating exceptions from log events in Symantec Endpoint Protection Manager”](#) on page 511.
- Delete files from the **Quarantine**.
See [“Using the Risk log to delete quarantined files on your client computers”](#) on page 449.

[Table 25-3](#) describes the different types of content that you can view and the actions that you can take from each log.

Table 25-3 Log types

Log type	Contents and actions
Audit	<p>The Audit log contains information about policy modification activity.</p> <p>Available information includes the event time and type; the policy modified; the domain, site, and user name involved; and a description.</p> <p>No actions are associated with this log.</p>
Application and Device Control	<p>The Application Control log and the Device Control log contain information about events where some type of behavior was blocked.</p> <p>The following Application and Device Control logs are available:</p> <ul style="list-style-type: none"> ■ Application Control, which includes information about Tamper Protection ■ Device Control <p>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.</p> <p>You can create an application control or Tamper Protection exception from the Application Control log.</p> <p>See “Specifying how Symantec Endpoint Protection handles monitored applications on Windows clients” on page 507.</p>
Compliance	<p>The compliance logs contain information about client Host Integrity.</p> <p>No actions are associated with these logs.</p>

Table 25-3 Log types (continued)

Log type	Contents and actions
Computer Status	<p>The Computer Status log contains information about the real-time operational status of the client computers in the network.</p> <p>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.</p> <p>You can also clear the infected status of computers from this log.</p> <p>Note: This log contains information that is collected from both Windows clients and Mac clients.</p>
Network Threat Protection	<p>The Network Threat Protection logs contain information about attacks on the firewall and on intrusion prevention. Information is available about denial-of-service attacks, port scans, and the changes that were made to executable files. They also contain information about the connections that are made through the firewall (traffic), and the data packets that pass through. These logs also contain some of the operational changes that are made to computers, such as detecting network applications, and configuring software.</p> <p>No actions are associated with these logs.</p>
SONAR	<p>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.</p> <p>The information includes items such as the time of occurrence, event actual action, user name, Web domain, application, application type, file, and path.</p> <p>If you have 11.0 clients in your network, the SONAR log can also contain information from legacy TruScan proactive threat scans.</p> <p>See "About SONAR" on page 484.</p>
Risk	<p>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.</p>
Scan	<p>The Scan log contains information about virus and spyware scan activity from both Windows clients and Mac clients.</p> <p>Available information includes items such as the scan start, computer, IP address, status, duration, detections, scanned, omitted, and domain.</p> <p>No actions are associated with these logs.</p>

Table 25-3 Log types (continued)

Log type	Contents and actions
System	The system logs contain information about events such as when services start and stop. No actions are associated with these logs.

Saving and deleting custom logs by using filters

You can construct custom filters by using the **Basic Settings** and **Advanced Settings** to change the information that you want to see. You can save your filter settings to the database so that you can generate the same view again in the future. When you save your settings, they are saved in the database. The name you give to the filter appears in the **Use a saved filter** list box for that type of logs and reports.

Note: If you selected **Past 24 hours** as the time range for a log filter, the 24-hour time range begins when you first select the filter. If you refresh the page, the start of the 24-hour range does not reset. If you select the filter, and wait to view a log, the time range starts when you select the filter. It does not start when you view the log.

If you want to make sure the past 24-hour range starts now, select a different time range and then reselect **Past 24 hours**.

To save a custom log by using a filter

- 1 In the main window, click **Monitors**.
- 2 On the **Logs** tab, select the type of log view that you want to configure a filter for from the **Log type** list box.
- 3 For some types of logs, a **Log content** list box appears. If it appears, select the log content that you want to configure a filter for.
- 4 In the **Use a saved filter** list box, select the filter that you want to start from. For example, select the default filter.
- 5 Under **What filter settings would you like to use**, click **Advanced Settings**.
- 6 Change any of the settings.
- 7 Click **Save Filter**.
- 8 In the dialog box that appears, in the **Filter name** box, type the name that you want to use for this log filter configuration. Only the first 32 characters of the name that you give display when the saved filter is added to the filter list.

- 9 Click **OK** and your new filter name is added to the **Use a saved filter** list box.
- 10 When the confirmation dialog box appears, click **OK**.

To delete a saved filter

- 1 In the **Use a saved filter** list box, select the name of the log filter that you want to delete.
- 2 Beside the **Use a saved filter** list box, click the **Delete** icon.
- 3 When you are prompted to confirm that you want to delete the filter, click **Yes**.

Viewing logs from other sites

If you want to view the logs from another site, you must log on to a server at the remote site from the Symantec Endpoint Protection Manager console. If you have an account on a server at the remote site, you can log on remotely and view that site's logs.

If you have configured replication partners, you can choose to have all the logs from the replication partners copied to the local partner and vice versa.

See [“Specifying which data to replicate”](#) on page 729.

If you choose to replicate logs, by default you see the information from both your site and the replicated sites when you view any log. If you want to see a single site, you must filter the data to limit it to the location you want to view.

Note: If you choose to replicate logs, be sure that you have sufficient disk space for the additional logs on all the Replication Partners.

To view the logs from another site

- 1 Open a Web browser.
- 2 Type the server name or IP address and the port number, 9090, in the address text box as follows:

http://192.168.1.100:9090

The console then downloads. The computer from which you log on must have the Java 2 Runtime Environment (JRE) installed. If it does not, you are prompted to download and install it. Follow the prompts to install the JRE.

- 3 In the console logon dialog box, type your user name and password.

- 4 In the **Server** text box, if it does not fill automatically, type the server name or IP address and port number 8443 as follows:

http://192.168.1.100:8443

- 5 Click **Log On**.

Managing notifications

This chapter includes the following topics:

- [Managing notifications](#)
- [Establishing communication between the management server and email servers](#)
- [Viewing and acknowledging notifications](#)
- [Saving and deleting administrative notification filters](#)
- [Setting up administrator notifications](#)
- [How upgrades from another version affect notification conditions](#)

Managing notifications

Notifications alert administrators and computer users about potential security problems.

Some notification types contain default values when you configure them. These guidelines provide reasonable starting points depending on the size of your environment, but they may need to be adjusted. Trial and error may be required to find the right balance between too many and too few notifications for your environment. Set the threshold to an initial limit, then wait for a few days. After a few days, you can adjust the notifications settings.

For virus, security risk, and firewall event detection, suppose that you have fewer than 100 computers in a network. A reasonable starting point in this network is to configure a notification when two risk events are detected within one minute. If you have 100 to 1000 computers, detecting five risk events within one minute may be a more useful starting point.

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

Table 26-1 lists the tasks you can perform to manage notifications.

Table 26-1 Notification management

Task	Description
Learn about notifications	Learn how notifications work. See “How notifications work” on page 621.
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 628.
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 622.
View unacknowledged notifications	View and respond to unacknowledged notifications. See “Viewing and acknowledging notifications” on page 628.
Configure new notifications	Optionally create notifications to remind you and other administrators about important issues. See “Setting up administrator notifications” on page 630. See “About turning on notifications for remote clients” on page 288.
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 630.

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 a large-scale virus attack occurs, and that there is a notification condition configured to send an email whenever viruses infect five computers on the network. If you set a one hour damper period for that notification condition, the server sends only one notification email each hour during the attack.

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 620.

See [“Establishing communication between the management server and email servers”](#) on page 628.

See [“What are the types of notifications and when are they sent?”](#) on page 622.

See [“Setting up administrator notifications”](#) on page 630.

See [“Viewing and acknowledging notifications”](#) on page 628.

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 620.

See [“How upgrades from another version affect notification conditions”](#) on page 632.

Table 26-2 Preconfigured notifications

Notification	Description
<p>Authentication failure</p>	<p>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.</p>
<p>Client list changed</p>	<p>This notification triggers when there is a change to the existing client list. This notification condition is enabled by default.</p> <p>Client list changes can include:</p> <ul style="list-style-type: none"> ■ 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 <p>This notification is enabled by default.</p>
<p>Client security alert</p>	<p>This notification triggers upon any of the following security events:</p> <ul style="list-style-type: none"> ■ Compliance events ■ Network Threat Protection events ■ Traffic events ■ Packet events ■ Device control events ■ Application control events <p>You can modify this notification to specify the type, severity, and frequency of events that determine when these notifications are triggered.</p> <p>Some of these occurrence types require that you also enable logging in the associated policy.</p> <p>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.</p>

Table 26-2 Preconfigured notifications (*continued*)

Notification	Description
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.
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. The Paid License Issue notification is enabled by default.
Licensing issue Over-deployment	This notification alerts administrators and, optionally, partners, about over-deployed paid licenses. The Over Deployment Issue notification is enabled by default.
Licensing issue Trial license expiration	This notification alerts administrators about expired trial licenses and the trial licenses that are due to expire in 60, 30, and 7 days. This notification is enabled by default if there is a trial license. It is not enabled by default if your license is due for an upgrade or has been paid.

Table 26-2 Preconfigured notifications (*continued*)

Notification	Description
<p>Network load alert: requests for full definitions</p>	<p>Alerts the administrators when too many clients request a full definition set, and to potential network bandwidth issues.</p> <p>The Network Load: Requests for Full Definitions notification is enabled by default.</p>
<p>New learned application</p>	<p>This notification triggers when application learning detects a new application.</p>
<p>New risk detected</p>	<p>This notification triggers whenever virus and spyware scans detect a new risk.</p> <p>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.</p>
<p>New software package</p>	<p>This notification triggers when a new software package downloads or the following occurs:</p> <ul style="list-style-type: none"> ■ LiveUpdate downloads a client package. ■ The management server is upgraded. ■ The console manually imports client packages. <p>You can specify whether the notification is triggered only by new security definitions, only by new client packages, or by both. By default, the Client package setting option is enabled and the Security definitions option is disabled for this condition.</p> <p>The New Client Software notification is enabled by default.</p>
<p>New user-allowed download</p>	<p>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.</p>
<p>Power Eraser recommended</p>	<p>Alerts the administrators when a regular scan cannot repair an infection, so the administrators can use Power Eraser.</p> <p>This notification is enabled by default.</p>

Table 26-2 Preconfigured notifications (*continued*)

Notification	Description
Risk outbreak	<p>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.</p> <p>This notification condition is enabled by default.</p> <p>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.</p>
Security Virtual Appliance offline	<p>This notification alerts administrators when a Security Virtual Appliance goes offline. Security Virtual Appliances run only in VMware vShield infrastructures.</p>
Server health	<p>Server health issues trigger the notification. The notification lists the server name, the health status, the reason, and the last online or offline status.</p> <p>This notification is enabled by default.</p>
Single risk event	<p>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.</p> <p>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.</p>
SONAR definition out-of-date	<p>Alerts the administrators about out-of-date SONAR definitions. You can specify the age at which the definitions trigger the notification.</p>

Table 26-2 Preconfigured notifications (*continued*)

Notification	Description
System event	<p>This notification triggers upon certain system events and provides the number of such events that were detected.</p> <p>System events include the following events:</p> <ul style="list-style-type: none"> ■ Server activities ■ Replication failures ■ System errors
Unmanaged computers	<p>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.</p>
Upgrade license expiration	<p>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.</p> <p>Note: The Upgrade license expiration notification appears only after a Symantec Endpoint Protection upgrade.</p>
Virus definitions out-of-date	<p>Alerts the administrators about out-of-date virus definitions. You can specify the age at which the definitions trigger the notification.</p> <p>This notification is enabled by default.</p>

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 622.

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 620.

To establish communication between the management server and email servers

- 1 In the console, click **Admin**, and then click **Servers**.
- 2 Under **Servers**, select the management server for which you want to establish a connection to the email server.
- 3 Under **Tasks**, click **Edit the server properties**.
- 4 In the **Server Properties** dialog box, click the **Email Server** tab.
- 5 Enter the email server settings.

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

- 6 Click **OK**.

Viewing and acknowledging notifications

You can view unacknowledged notifications or all notifications. You can acknowledge an unacknowledged notification. You can view all the notification conditions that are currently configured in the console.

The **Security Status** pane on the **Home** page indicates the number of unacknowledged notifications that have occurred during the last 24 hours.

See [“Managing notifications”](#) on page 620.

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 630.
- 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 629.
 See [“To view all notifications”](#) on page 629.
- 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 628.

See [“Managing notifications”](#) on page 620.

You can create a saved filter that uses any combination of the following criteria:

- **Time range**
- **Acknowledged status**
- **Notification type**
- **Created by**
- **Notification name**

For example, you can create a filter that only displays unacknowledged risk outbreak notifications posted during the past 24 hours.

To add a notification filter

- 1 In the console, click **Monitors**.
- 2 On the **Monitors** page, on the **Notifications** tab, click **Advanced Settings**.
- 3 Under the **What filter settings would you like to use?** heading, set the criteria for the filter.
- 4 Click **Save Filter**.
- 5 On the **Notifications** tab, in the **Filter name** box, type a filter name, and then click **OK**.

To delete a saved notification filter

- 1 In the console, click **Monitors**.
- 2 On the **Monitors** page, on the **Notifications** tab, on the **Use a saved filter** menu, choose a filter.
- 3 At the right of the **Use a saved filter** menu, click the **X** icon.
- 4 In the **Delete Filter** dialog box, click **Yes**.

Setting up administrator notifications

You can configure notifications to alert you and other administrators when particular kinds of events occur. You can also add the conditions that trigger notifications to remind you to perform important tasks. For example, you can add a notification

condition to inform you when a license has expired, or when a security risk has been detected.

When 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 628.

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 620.

See [“Viewing and acknowledging notifications”](#) on page 628.

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 622.

Protecting clients in virtual environments

- [Chapter 27. Overview of Symantec Endpoint Protection and virtual infrastructures](#)
- [Chapter 28. Installing and using a network-based Shared Insight Cache](#)
- [Chapter 29. Installing a Security Virtual Appliance and using a vShield-enabled Shared Insight Cache](#)
- [Chapter 30. Using Virtual Image Exception](#)
- [Chapter 31. Non-persistent virtual desktop infrastructures](#)

Overview of Symantec Endpoint Protection and virtual infrastructures

This chapter includes the following topics:

- [Using Symantec Endpoint Protection in virtual infrastructures](#)
- [About Shared Insight Cache](#)
- [About the Virtual Image Exception tool](#)

Using Symantec Endpoint Protection in virtual infrastructures

Symantec Endpoint Protection provides the Shared Insight Cache and Virtual Image Exception features for virtual infrastructures, which you can enable to improve performance. You need to perform some additional installation and configuration tasks to enable these features.

Table 27-1 Virtual infrastructure features and their use

Feature and use	Description
<p>Use Shared Insight Cache to skip the scanning of files that are known to be clean.</p>	<p>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.</p> <p>You can set up the following types of Shared Insight Cache:</p> <ul style="list-style-type: none"> ■ A vShield-enabled Shared Insight Cache Virtual clients in a VMware vShield infrastructure can use a vShield-enabled Shared Insight Cache reduce scan loads. ■ A network-based Shared Insight Cache Virtual clients that use any kind of virtual infrastructure can use a network-based Shared Insight Cache reduce scan loads. <p>Note: Symantec supports the use of the vShield-enabled Shared Insight Cache only for VMware infrastructures.</p> <p>See “About Shared Insight Cache” on page 637.</p> <p>See “What do I need to do to use a vShield-enabled Shared Insight Cache?” on page 653.</p> <p>See “What do I need to do to use a network-based Shared Insight Cache?” on page 639.</p>
<p>Use the Virtual Image Exception tool so that clients can skip the scanning of base image files.</p>	<p>The Virtual Image Exception tool lets you mark base image files as safe so that scans skip those files to reduce scan loads.</p> <p>Note: Symantec does not support the use of the Virtual Image Exception tool in a physical environment.</p> <p>See “About the Virtual Image Exception tool” on page 638.</p>
<p>Configure the non-persistent virtual desktop infrastructures feature.</p>	<p>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.</p> <p>See “Using Symantec Endpoint Protection in non-persistent virtual desktop infrastructures” on page 675.</p> <p>See “Configuring a separate purge interval for offline non-persistent VDI clients” on page 678.</p>

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 639.

See [“Customizing network-based Shared Insight Cache configuration settings”](#) on page 644.

See [“What do I need to do to install a Security Virtual Appliance?”](#) on page 654.

See [“What do I need to do to use a vShield-enabled Shared Insight Cache?”](#) on page 653.

See [“Using Symantec Endpoint Protection in virtual infrastructures”](#) on page 635.

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 671.

See [“Using Symantec Endpoint Protection in virtual infrastructures”](#) on page 635.

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?](#)
- [System requirements for implementing a network-based Shared Insight Cache](#)
- [Installing and uninstalling a network-based Shared Insight Cache](#)
- [Enabling or disabling the use of a network-based Shared Insight Cache](#)
- [Customizing network-based Shared Insight Cache configuration settings](#)
- [About stopping and starting the network-based Shared Insight Cache service](#)
- [Viewing network-based Shared Insight Cache log events](#)
- [Monitoring network-based Shared Insight Cache performance counters](#)
- [Troubleshooting issues with Shared Insight Cache](#)

What do I need to do to use a network-based Shared Insight Cache?

You can use a network-based Shared Insight Cache to improve scan performance.

Table 28-1 Tasks to install and use a network-based Shared Insight Cache

Step	Task
Step 1	<p>Install Shared Insight Cache.</p> <p>See “System requirements for implementing a network-based Shared Insight Cache” on page 640.</p> <p>See “Installing and uninstalling a network-based Shared Insight Cache” on page 641.</p>
Step 2	<p>In the Virus and Spyware policy in Symantec Endpoint Protection Manager, enable your virtual clients to use Shared Insight Cache.</p> <p>See “Enabling or disabling the use of a network-based Shared Insight Cache” on page 643.</p>

After you have installed a Shared Insight Cache, you can optionally do the following tasks:

- Customize any of the service, cache, or log settings for Shared Insight Cache. See [“Customizing network-based Shared Insight Cache configuration settings”](#) on page 644.
- View related events in the log. See [“Viewing network-based Shared Insight Cache log events”](#) on page 648.
- Use the Windows Performance Manager to monitor its performance. See [“Monitoring network-based Shared Insight Cache performance counters”](#) on page 650.

System requirements for implementing a network-based Shared Insight Cache

[Table 28-2](#) describes the minimum system requirements that a virtual infrastructure needs to run Shared Insight Cache.

Table 28-2 Network-based Shared Insight Cache system requirements

Requirement	Description
Software	<ul style="list-style-type: none"> ■ Windows Server 2003 (12.1 through 12.1.4 only) ■ Windows Server 2008 and later ■ Windows Server 2012 and Windows Server 2012 R2 (as of 12.1.5) ■ .NET Framework 4

Table 28-2 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 637.

See [“Installing and uninstalling a network-based Shared Insight Cache”](#) on page 641.

Installing and uninstalling a network-based Shared Insight Cache

Before you install Shared Insight Cache, ensure that you have met all the system requirements and that you are logged on as a Windows administrator.

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 640.

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 network-based Shared Insight Cache configuration settings”](#) on page 644.

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 648.

Note: To uninstall the Shared Insight Cache, use the appropriate Windows control panel, such as Add or Remove Programs. You must have Windows administrator rights to uninstall Shared Insight Cache.

If you uninstall Shared Insight Cache, you may also want to disable the Shared Insight Cache in Symantec Endpoint Protection Manager. Disabling Shared Insight Cache prevents the Windows Event log from receiving notifications each time clients cannot contact the cache.

Enabling or disabling the use of a network-based Shared Insight Cache

For communication over the network, by default Shared Insight Cache uses no authentication and no SSL. The default setting for the password is null. In other words, the password is blank. If you change Shared Insight Cache settings to Basic authentication with SSL or Basic authentication with no SSL, you must specify a user name and password that can access Shared Insight Cache.

You can also change a user-defined authentication password. But if you do, you must specify that authentication user name and password in Symantec Endpoint Protection Manager so that clients can communicate with Shared Insight Cache.

To enable the use of a network-based Shared Insight Cache

- 1 In the Symantec Endpoint Protection Manager console, open the appropriate Virus and Spyware Protection policy and click **Miscellaneous**.
- 2 Click the **Shared Insight Cache** tab.
- 3 Check **Enable Shared Insight Cache**.
- 4 Click **Shared Insight Cache using the network**.
- 5 If you enabled SSL as a part of the Shared Insight Cache server settings in the configuration file, then click **Require SSL**.

If you enable SSL, you must also set up your clients to communicate with Shared Insight Cache by adding the Shared Insight Cache server certificate to the trusted certificates authorities store for the local computer. Otherwise, the communication between the clients and the Shared Insight Cache fails.

For information about how to add a server certificate, see your Active Directory documentation.

- 6 In the **Hostname** box, type the host name of the host on which you installed Shared Insight Cache.
- 7 In the **Port** box, type the port number of Shared Insight Cache.
- 8 Optionally, if you configured authentication for Shared Insight Cache, in the **Username** box, type the user name.
- 9 Optionally, if you configured authentication for Shared Insight Cache, click **Change Password** to change the default password (null) to the password that you created for authentication.

- 10 In the **New password** and the **Confirm password** boxes, type the new password.

Leave these fields empty if you do not want to use a password.

- 11 Click **OK**.

See [“What do I need to do to use a network-based Shared Insight Cache?”](#) on page 639.

To disable the use of a network-based Shared Insight Cache

- 1 In the Symantec Endpoint Protection Manager console, open the appropriate Virus and Spyware Protection policy and click **Miscellaneous**.
- 2 Click the **Shared Insight Cache** tab.
- 3 Uncheck **Enable Shared Insight Cache**.
- 4 Click **OK**.

Customizing network-based Shared Insight Cache configuration settings

After you install Shared Insight Cache, you can customize its settings in the configuration file.

The configuration file is an XML file that follows .NET Framework application configuration standards. Shared Insight Cache does not start if there is an invalid configuration, such as invalid XML, incorrect value types, or missing required values.

For more information, see:

[Configuration Editor Tool \(SvcConfigEditor.exe\)](#)

[Table 28-3](#) describes the options that you can configure.

Table 28-3 Shared Insight Cache configuration options

Option and default value	Description and comments
<p>Cache Service Listening Port</p> <p>The default value is 9005.</p>	<p>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.</p> <p>If the range for the port is not between 0 - 65535, the service does not start.</p> <p>The service does not start if it cannot listen on the specified port.</p> <pre><endpoint address="http://localhost:9005/1"</pre> <p>By default, the Shared Insight Cache server listens on all IP addresses. To configure the listening IP addresses for HTTP or HTTPS services, you must use HttpCfg.exe (Windows 2003) or Netsh.exe (Windows 2008). The Shared Insight Cache server listens on the IP addresses that you specified in the IP Listen List modified by those tools.</p> <p>Netsh.exe is included with Windows 2008. You can install HttpCfg.exe from the Windows 2003 installation disc. The installer is located at the following path: \Support\Tools\Suptools.msi</p> <p>For more information, see: Configuring HTTP and HTTPS</p>
<p>Status Service Listening Port</p> <p>The default value is 9006.</p>	<p>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.</p> <p>The service does not start if the range is not between 0 - 65535.</p> <p>The service does not start if it cannot listen on the specified port.</p>
<p>Vote Count</p> <p>The default value is 1.</p>	<p>Number of the clients that must verify that the file is clean before Shared Insight Cache uses the results.</p> <p>The value must be less than or equal to 15. If the value is greater than 15, the server uses the default value.</p> <pre><cache.configuration vote.count="1"</pre>
<p>Prune Size</p> <p>The default value is 10.</p>	<p>Percentage of memory usage to remove from the cache when the cache hits the memory usage limit.</p> <p>The value must be between 10 and 100. If the value is not between 10 and 100, the server uses the default value.</p> <p>Note: Symantec recommends that you keep the default prune size.</p> <pre>prune.size="10"</pre>

Table 28-3 Shared Insight Cache configuration options (*continued*)

Option and default value	Description and comments
<p>Memory Usage</p> <p>The default value is 50.</p>	<p>Percentage of size of the cache before Shared Insight Cache starts pruning the cache. Must be greater than or equal to 10.</p> <pre>mem.usage="50"</pre>
<p>Log File</p> <p>The default value is <i>install_folder/CacheServer.log</i></p>	<p>A file for the Shared Insight Cache log.</p> <pre><filevalue="CacheServer.log" /></pre>
<p>Log Level</p> <p>The default value is ERROR.</p>	<p>ALL DEBUG INFO WARN ERROR FATAL OFF</p> <p>A value of OFF indicates that Shared Insight Cache does not log any messages.</p> <pre><level value="ERROR" /></pre> <p>See "Viewing network-based Shared Insight Cache log events" on page 648.</p>
<p>Log Size</p> <p>The default value is 10000.</p>	<p>Size of the log (in bytes) until Shared Insight Cache rolls the log over.</p> <pre><maximumFileSizevalue="10000" /></pre>
<p>Log Backups</p> <p>The default value is 1.</p>	<p>Number of rolled over logs to keep before the oldest log is deleted.</p> <p>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.</p> <pre><maxSizeRollBackupsvalue="1" /></pre>

Table 28-3 Shared Insight Cache configuration options (*continued*)

Option and default value	Description and comments
<p>Enable SSL</p> <p>Enable authentication</p>	<p>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.</p> <pre><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></pre> <p>See "Enabling or disabling the use of a network-based Shared Insight Cache" on page 643.</p>

To customize Shared Insight Cache settings

- 1 Navigate to and open the following file:

Installation folder\SharedInsightCacheInstallation.exe.config

- 2 Make the modifications as needed.

- 3 Save your changes and close the file.
- 4 Restart the Shared Insight Cache service.

You must restart the Shared Insight Cache service for changes to all configuration settings except the log level to take effect.

See [“About stopping and starting the network-based Shared Insight Cache service”](#) on page 648.

See [“What do I need to do to use a network-based Shared Insight Cache?”](#) on page 639.

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 651.

Viewing network-based Shared Insight Cache log events

You can view the Shared Insight Cache log file to see any events that Shared Insight Cache creates. The log file is located in the installation folder and is named `CacheServer.log`.

Shared Insight Cache prints logs in the following format:

```
[[] %thread | %d{MM/dd/yyyyHH:mm:ss} | %level | %logger{2} | %message [-]%newline
```

For example:

```
[[] 4 | 12/15/2010 10:51:37 | INFO | CacheServerService.Service | Started service [-]
```

Modify the configuration file to specify the log level that you want to use for network-based Shared Insight Cache.

Table 28-4 describes the levels that you can set.

Table 28-4 Network-based Shared Insight Cache log levels

Log level	Description
OFF	OFF indicates that no incidents are logged.
FATAL	FATAL messages require you to take action. These messages are the errors that cause Shared Insight Cache to stop. For example, a FATAL message may indicate that the server IP address is not available, which means that Shared Insight Cache cannot run.
ERROR	ERROR messages require you to take action, but the process continues to run. They are errors in the system that cause Shared Insight Cache to fail or lose functionality. You also receive all log entries for FATAL messages. This level is the default logging level.
WARN	WARN messages indicate Shared Insight Cache behavior that may be undesirable, but do not cause it to fail. You also receive all log entries for FATAL messages and ERROR messages.
INFO	INFO messages describe the general actions of or give information about Shared Insight Cache. They may indicate the state of the system and help validate behavior or track down issues. However, alone they are not intended to report actionable items. For example, an information message may indicate that cache pruning is complete. The message does not detail a problem. It only logs behavior. You also receive all log entries for FATAL messages, ERROR messages, and WARN messages.
DEBUG ALL	DEBUG and ALL log level messages produce the same results. These log levels are intended for Support to troubleshoot problems with Shared Insight Cache. You also receive all log entries for all other log levels.

Increase the log level only when you need to troubleshoot issues with Shared Insight Cache. When you increase the log level, you begin to significantly increase the size of the log file. When you resolve the issue, return to the default log level of ERROR.

To view Shared Insight Cache events in the log

- ◆ Go to the following location:

Installation folder/CacheServer.log

See [“Customizing network-based Shared Insight Cache configuration settings”](#) on page 644.

Monitoring network-based Shared Insight Cache performance counters

You can view network-based Shared Insight Cache statistics in the Windows Performance Monitor. The Shared Insight Cache service must be running to view its performance counters.

Table 28-5 Shared Insight Cache statistics

Statistic	Description
The number of items in the cache	This number represents the current number of items in the cache.
The number of items in the cache that have been voted clean	This number represents the current number of items in the cache, which have been voted clean.
Number of cache requests	The number of cache requests that have been made to the Shared Insight Cache service. This number includes only the number of valid requests that received a 200 response. This counter does not persist across restarts of the service.
Number of update requests	The number of update requests that have been made to the service. This number is only the valid requests that received a 200 response. This counter does not persist across restarts of the service.

To monitor network-based Shared Insight Cache performance counters

- 1 At the command prompt, type the following command:

`perfmon`
- 2 In the **Performance** window, right-click the graph.
- 3 Select **Add Counters**.
- 4 In the **Performance object** drop-down list, select **Shared Insight Cache**.

5 Select the counters that you want to view, and click **Add**.

6 Click **Close**.

The Shared Insight Cache counters that you selected appear in the Performance graph.

For more information about using the Windows performance monitor, see your Windows documentation.

See [“Troubleshooting issues with Shared Insight Cache”](#) on page 651.

See [“What do I need to do to use a network-based Shared Insight Cache?”](#) on page 639.

Troubleshooting issues with Shared Insight Cache

[Table 28-6](#) provides suggestions for how to troubleshoot issues with Shared Insight Cache.

Table 28-6 Troubleshooting Shared Insight Cache

Issue	Explanation/Resolution
Experiencing problems with the cache results	Restart the service. See “About stopping and starting the network-based Shared Insight Cache service” on page 648.
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: <code>%Windir%\System32\Logfiles\HTTPERR</code>

See [“Viewing network-based Shared Insight Cache log events”](#) on page 648.

See [“Monitoring network-based Shared Insight Cache performance counters”](#) on page 650.

Installing a Security Virtual Appliance and using a vShield-enabled Shared Insight Cache

This chapter includes the following topics:

- [What do I need to do to use a vShield-enabled Shared Insight Cache?](#)
- [What do I need to do to install a Security Virtual Appliance?](#)
- [About the Symantec Endpoint Protection Security Virtual Appliance](#)
- [VMware software requirements to install a Symantec Security Virtual Appliance](#)
- [VMware software requirements for the Guest Virtual Machines](#)
- [Configuring the Symantec Endpoint Protection Security Virtual Appliance installation settings file](#)
- [Installing a Symantec Endpoint Protection Security Virtual Appliance](#)
- [Enabling Symantec Endpoint Protection clients to use a vShield-enabled Shared Insight Cache](#)
- [Stopping and starting the vShield-enabled Shared Insight Cache service](#)
- [Service commands for the vShield-enabled Shared Insight Cache](#)
- [Configuration file settings for a vShield-enabled Shared Insight Cache](#)
- [About vShield-enabled Shared Insight Cache event logging](#)

- [Uninstalling a Symantec Endpoint Protection Security Virtual Appliance](#)

What do I need to do to use a vShield-enabled Shared Insight Cache?

A vShield-enabled Shared Insight Cache runs in a Symantec Endpoint Protection Security Virtual Appliance. Windows-based Guest Virtual Machines (GVMs) use VMware vShield Endpoint to access the Shared Insight Cache.

Note: Symantec supports the use of a vShield-enabled Shared Insight Cache only in VMware ESX/ESXi infrastructures.

Table 29-1 Tasks that you need to perform to use a vShield-enabled Shared Insight Cache

Step	Task
Step 1	Install a Security Virtual Appliance on an ESX/ESXi host. See “What do I need to do to install a Security Virtual Appliance?” on page 654.
Step 2	Install the VMware EPSEC driver on each GVM so that they can communicate with the Security Virtual Appliance. See “VMware software requirements for the Guest Virtual Machines” on page 658.
Step 3	Enable the GVMs (clients) to use Shared Insight Cache. You perform this task from the Virus and Spyware Protection policy in the Symantec Endpoint Protection Manager. See “Enabling Symantec Endpoint Protection clients to use a vShield-enabled Shared Insight Cache” on page 665.

After you enable GVM clients to use a vShield-enabled Shared Insight Cache, you can optionally configure administrator notifications for Security Virtual Appliances that go offline.

See [“Setting up administrator notifications”](#) on page 630.

What do I need to do to install a Security Virtual Appliance?

A vShield-enabled Shared Insight Cache runs in a Symantec Endpoint Protection Security Virtual Appliance. You must install the appliance so that Windows-based Guest Virtual Machines (GVMs) can use VMware vShield Endpoint to access the Shared Insight Cache.

Note: Symantec supports the use of the Security Virtual Appliance only in VMware ESX/ESXi infrastructures.

Table 29-2 Tasks that you need to perform to install a Symantec Endpoint Protection Security Virtual Appliance

Step	Task
Step 1	<p>Install and configure the prerequisite VMware software that you need.</p> <p>See “VMware software requirements to install a Symantec Security Virtual Appliance” on page 657.</p> <p>For information about how to install and configure VMware software, refer to your VMware documentation.</p>
Step 2	<p>Download the following files from FileConnect, at the following location: https://fileconnect.symantec.com/</p> <ul style="list-style-type: none"> ■ The Symantec Endpoint Protection Tools installation file Extract the contents of the .exe file. Locate the <code>Virtualization\SecurityVirtualAppliance</code> folder. ■ The Symantec Endpoint Protection Security Virtual Appliance .ova Note: If you download the .ova file using Internet Explorer, the file is saved with a .man or .tar extension. You must rename the file with an .ova extension. <p>Copy the entire contents of the <code>SecurityVirtualAppliance</code> folder to a local directory. For convenience, save the .ova file to the same local directory.</p> <p>To access FileConnect, you need to have the activation serial number that is part of your license certificate.</p>

Table 29-2 Tasks that you need to perform to install a Symantec Endpoint Protection Security Virtual Appliance (*continued*)

Step	Task
Step 3	<p>In Symantec Endpoint Protection Manager, export the communication settings file (<code>sylink.xml</code>) from the client group that you plan to use for your Guest Virtual Machines (GVMs). You must have this file to install the Security Virtual Appliance.</p> <p>Note: Symantec recommends using the default communications settings of a heartbeat interval and randomization interval of 5 minutes each when you use the Security Virtual Appliance. If the group <code>sylink.xml</code> uses a longer interval, such as a one-hour heartbeat and a four-hour randomization, it could delay reporting for that group. You should export the <code>sylink.xml</code> for the Security Virtual Appliance before adjusting the communication settings for the virtual machine group.</p> <p>For convenience, save the <code>sylink.xml</code> file to the same local directory as the <code>.ova</code> file and the <code>SecurityVirtualAppliance</code> folder contents.</p> <p>The default name of the communications file that you exported from Symantec Endpoint Protection Manager is <code>group_name_sylink.xml</code>.</p> <p>See “Exporting the client-server communications file (Sylink.xml) manually” on page 176.</p>
Step 4	<p>Update the installation settings file with the information that the installation executable requires to install the Security Virtual Appliance on the ESXi host.</p> <p>See “Configuring the Symantec Endpoint Protection Security Virtual Appliance installation settings file” on page 658.</p>
Step 5	<p>Install the Security Virtual Appliance on the ESX/ESXi host.</p> <p>See “Installing a Symantec Endpoint Protection Security Virtual Appliance” on page 662.</p>

After you install a Security Virtual Appliance, you can enable a vShield-enabled Shared Insight Cache for your GVMs to use.

See [“What do I need to do to use a vShield-enabled Shared Insight Cache?”](#) on page 653.

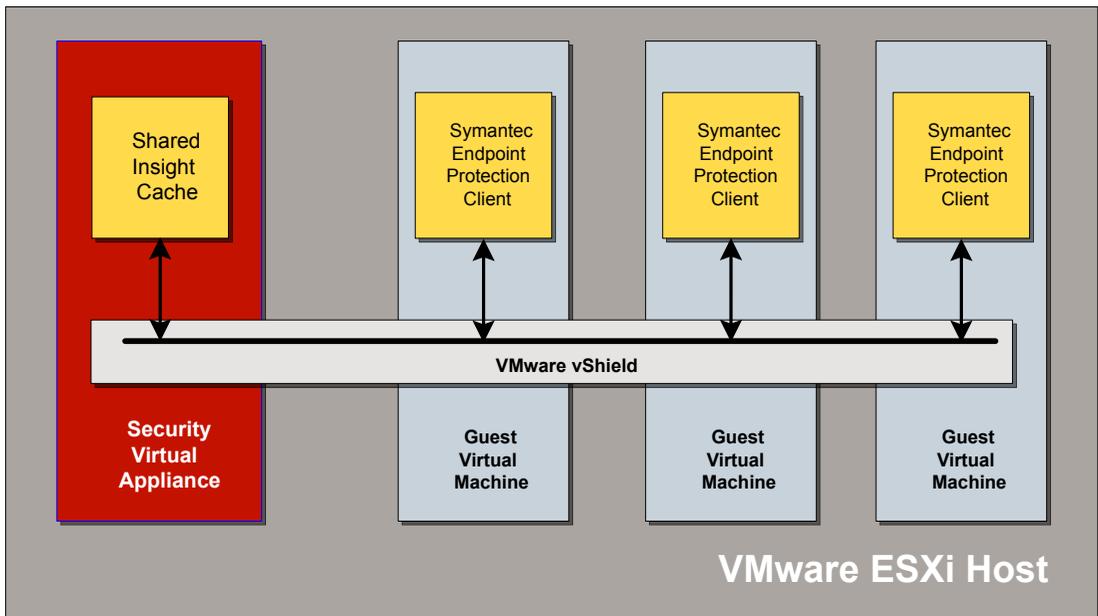
About the Symantec Endpoint Protection Security Virtual Appliance

The Symantec Endpoint Protection Security Virtual Appliance is a Linux-based virtual appliance that you install on a VMware ESX/ESXi server. The Security Virtual Appliance integrates with VMware’s vShield Endpoint. The Shared Insight Cache runs in the appliance and lets Windows-based Guest Virtual Machines (GVMs) with the Symantec Endpoint Protection client installed share scan results. Identical files are trusted and therefore skipped across all of the GVMs on the ESX/ESXi host.

Shared Insight Cache improves full scan performance by reducing disk I/O and CPU usage.

Note: You must install a Security Virtual Appliance on each ESX/ESXi host if you want the GVMs to access Shared Insight Cache.

Figure 29-1 Symantec Endpoint Protection Security Virtual Appliance architecture



The appliance is complete and ready to use as soon as you install it. The appliance includes the Shared Insight Cache.

See [“About Shared Insight Cache”](#) on page 637.

See [“VMware software requirements to install a Symantec Security Virtual Appliance”](#) on page 657.

See [“What do I need to do to install a Security Virtual Appliance?”](#) on page 654.

VMware software requirements to install a Symantec Security Virtual Appliance

[Table 29-3](#) describes the VMware components that you must have installed before you can install a Security Virtual Appliance. Once you have installed the appliance, you can enable a vShield-enabled Shared Insight Cache for the Guest Virtual Machines to use.

Table 29-3 VMware software requirements and prerequisites for installing a Security Virtual Appliance

Requirement	Description
VMware ESXi server software	<p>One of the following versions:</p> <ul style="list-style-type: none"> ■ ESX 4.1, with Patch ESX410-201107001 ■ ESXi 5.0 Update 1 ■ ESXi 5.1 ■ ESXi 5.1 Update 1
VMware vShield product software	<ul style="list-style-type: none"> ■ VMware vShield Manager 5.0 Update 1 ■ VMware vShield Endpoint 5.0 Update 1 ■ VMware vShield Manager 5.1 ■ VMware vShield Endpoint 5.1 <p>Note: You must use vShield Manager 5.0 Update 1 or later to deploy vShield Endpoint 5.0 Update 1 to each host you want to manage.</p> <p>For more information about using VMware vShield Endpoint 5.0 Update 1 with ESX 4.1, see the following web page:</p> <p>Using vShield Endpoint 5.0 and vShield Data Security 5.0 with vSphere 4.1</p>

Note: The Java Runtime Environment 7 or later is required to run the Security Virtual Appliance installation tool.

See [“Installing a Symantec Endpoint Protection Security Virtual Appliance”](#) on page 662.

See [“What do I need to do to install a Security Virtual Appliance?”](#) on page 654.

See [“VMware software requirements for the Guest Virtual Machines”](#) on page 658.

VMware software requirements for the Guest Virtual Machines

Table 29-4 describes the Guest Virtual Machines requirements to use the vShield-enabled Shared Insight Cache on the Symantec Security Virtual Appliance.

Table 29-4 VMware requirements for the Guest Virtual Machines

Requirement	Description
Guest Virtual Machines (GVMs)	<p>The EPSEC 2.0 driver must be installed on all GVMs.</p> <p>On GVMs hosted by ESX 4.1 with Patch ESX410-201107001 applied, download the EPSEC driver locally and execute the installer on the virtual machine.</p> <p>On GVMs hosted by ESXi 5.0 Update 1 or later, do one of the following:</p> <ul style="list-style-type: none">■ Download the EPSEC driver locally and execute the installer on the virtual machine.■ Use the VMware Tools installer to install the EPSEC driver. <p>Note: To install the EPSEC driver, perform a custom installation and select VMware Device Drivers > VMCI Driver > vShield Drivers or Guest Introspection Drivers.</p> <p>You can also perform a complete installation. Do not select the typical installation.</p>

See [“What do I need to do to use a vShield-enabled Shared Insight Cache?”](#) on page 653.

See [“VMware software requirements to install a Symantec Security Virtual Appliance”](#) on page 657.

Configuring the Symantec Endpoint Protection Security Virtual Appliance installation settings file

You must configure the `SVA_InstallSettings.xml` file before you can install the Security Virtual Appliance. This file is located in the `Tools\Virtualization\SecurityVirtualAppliance` folder of the extracted installation file.

Note: For convenience, copy the `SVA_InstallSettings.xml` file and `Symantec_SVA_Install.jar` file to the same local directory as the `.ova` file and `symlink.xml` file.

Note: All settings are mandatory for installation unless explicitly marked as optional.

Table 29-5 Security Virtual Appliance installation file settings

Setting	Description
VMware vCenter information <ul style="list-style-type: none"> ■ IP address ■ User name ■ Password 	<p>Set the VMware vCenter IP address, user name, and password for the Security Virtual Appliance installation.</p> <pre><vCenter> <ip_address>192.168.x.x</ip_address> <username>username</username> <!-- <password>password</password> --> </vCenter></pre> <p>Note: vCenter Administrator user name and password are required to install the Security Virtual Appliance. If you do not configure the password in this settings file, then the installation prompts you for the password.</p> <p>Note that to install or uninstall the Security Virtual Appliance, the vCenter Administrator account that you use must have permissions in the following privilege categories:</p> <ul style="list-style-type: none"> ■ Datastore (All privileges) ■ Network (All privileges) ■ vApp (All privileges) ■ Virtual Machine (All privileges) ■ Global > Cancel Task <p>You cannot set these permissions from the Symantec Endpoint Protection Security Virtual Appliance installation settings file.</p>

Table 29-5 Security Virtual Appliance installation file settings (*continued*)

Setting	Description
<p>VMware vShield Manager information</p> <ul style="list-style-type: none"> ■ IP address ■ User name ■ Password 	<p>Set the VMware vShield Manager IP address, user name, and password for the Security Virtual Appliance installation.</p> <p>Note: vShield Administrator credentials are required to install the Security Virtual Appliance. If you do not configure the password in this settings file, then the installation prompts you for the password.</p> <pre data-bbox="413 517 954 713"> <vShield> <ip_address>192.168.x.y</ip_address> <username>admin</username> <!-- <password>default</password> --> </vShield> </pre>

Table 29-5 Security Virtual Appliance installation file settings (*continued*)

Setting	Description
<p>Installation settings</p> <ul style="list-style-type: none"> ■ Symantec Endpoint Protection Security Virtual Appliance OVA file location ■ ESXi host IP address ■ <code>sylink.xml</code> file location ■ Datastore prompt 	<p>Provide the information that guides the Security Virtual Appliance installation:</p> <ul style="list-style-type: none"> ■ The installation package is the Symantec Endpoint Protection Security Virtual Appliance .ova file that you downloaded from FileConnect at https://symantec.flexnetoperations.com/. See “What do I need to do to install a Security Virtual Appliance?” on page 654. ■ The <code>sylink.xml</code> file contains the client group communication settings that you exported from Symantec Endpoint Protection Manager. The default name of the communications file that you exported from Symantec Endpoint Protection Manager is <code>group_name_sylink.xml</code>. Be sure to change the <code><sylink_xml></code> pathname in the <code>SVA_InstallSettings.xml</code> file to match your exported file name. See “Exporting the client-server communications file (Sylink.xml) manually” on page 176. <p>You can change the datastore prompt to zero if you want to install automatically on the first datastore for the ESXi host.</p> <pre data-bbox="413 829 1233 996"><Installation> <location_of_package>path to OVA file</location_of_package> <esx_ip_address>192.168.x.z</esx_ip_address> <sylink_xml>./sylink.xml</sylink_xml> <datastore_prompt>1</datastore_prompt> </Installation></pre> <p>For example, if you renamed the files to <code>sva.ova</code> and <code>svasylink.xml</code> and saved them to <code>C:\temp</code>, you would type:</p> <pre data-bbox="413 1107 1233 1274"><Installation> <location_of_package>c:/temp/sva.ova</location_of_package> <esx_ip_address>192.168.x.z</esx_ip_address> <sylink_xml>c:/temp/svasylink.xml</sylink_xml> <datastore_prompt>1</datastore_prompt> </Installation></pre>

Table 29-5 Security Virtual Appliance installation file settings (*continued*)

Setting	Description
<p>Security Virtual Appliance information</p> <ul style="list-style-type: none"> ■ SVA host name ■ SVA admin password ■ SVA network settings (Optional) <ul style="list-style-type: none"> ■ IP address ■ Gateway ■ Subnet ■ DNS 	<p>Set the Security Virtual Appliance host name. The host name must be unique within the vCenter. The host name is limited to alphanumeric characters and the hyphen character.</p> <p>The login account name for the Security Virtual Appliance is <code>admin</code>.</p> <p>Note: If you do not configure the admin account password in this settings file, then the installation prompts you for the password.</p> <p>Optionally, you can configure the Security Virtual Appliance network settings. By default the network settings are commented out and installation defaults to use DHCP. You are not required to use network settings to install a Security Virtual Appliance.</p> <p>Note: If you want to specify one of the Security Virtual Appliance network settings, you must uncomment and specify all four of them. If you specify only one to three of the network settings, the installation fails.</p> <pre data-bbox="413 769 1005 1142"><sva> <hostname>Symantec-SVA</hostname> <admin_password>symantec</admin_password> <!-- <ip_address>192.168.x.w</ip_address> <gateway>192.168.x.v</gateway> <subnet>255.255.255.0</subnet> <dns>192.168.x.u</dns> --> </sva></pre>

See [“Installing a Symantec Endpoint Protection Security Virtual Appliance”](#) on page 662.

See [“What do I need to do to install a Security Virtual Appliance?”](#) on page 654.

Installing a Symantec Endpoint Protection Security Virtual Appliance

After you have met the prerequisites, you can install the Security Virtual Appliance:

- Download the `.ova` file and `Virtualization\SecurityVirtualAppliance` folder contents.

See [“What do I need to do to install a Security Virtual Appliance?”](#) on page 654.

- Import the exported `sylink.xml` file.
See [“Exporting the client-server communications file \(Sylink.xml\) manually”](#) on page 176.
- Configured the `SVA_InstallSettings.xml` file.
See [“Configuring the Symantec Endpoint Protection Security Virtual Appliance installation settings file”](#) on page 658.

You use the Security Virtual Appliance installation tool from the command line. You must install a Security Virtual Appliance on each ESXi host if you want the GVMs on the host to use vShield-enabled Shared Insight Cache.

To install or uninstall the Security Virtual Appliance, the vCenter Administrator account that you use must have permissions in the following privilege categories:

- Datastore (All privileges)
- Network (All privileges)
- vApp (All privileges)
- Virtual Machine (All privileges)
- Global > Cancel Task

Note: As part of the installation process, the Security Virtual Appliance and its associated ESXi host registers with vShield Manager. For this reason, you should not use vMotion with the Security Virtual Appliance. A best practice is to use the `sva_install.jar` utility to uninstall and reinstall the Security Virtual Appliance.

See [“VMware software requirements to install a Symantec Security Virtual Appliance”](#) on page 657.

Note: The Java Runtime Environment 7 or later is required to run the Security Virtual Appliance installation tool.

To install a Security Virtual Appliance

- 1 Take a snapshot of the vShield Manager. During installation, the Security Virtual Appliance registers with the vShield Manager. A snapshot ensures that you can revert to the previous state, in case any Security Virtual Appliance installation issues occur.
- 2 At the command line, type the following command:

```
java -jar Symantec_SVA_Install.jar -s  
pathname/SVA_InstallSettings.xml
```

By default, if there is more than one datastore available the installation prompts you to select one. If there is more than one network, the installation prompts you to select one.

Errors and other installation output are written to the `SVA_Install.log` file. This log file is created in the same directory where you executed the installation command.

Note: In a few instances, the write to that directory may fail. In these cases, the file is written to the `/temp` directory and is named `SVA_Installxxx.log`, where the system replaces `xxx` with a random number.

You can perform the following actions to recover from an incomplete Security Virtual Appliance installation or an aborted Security Virtual Appliance installation.

To recover from an incomplete installation or an aborted installation

- 1 Check to see if the Security Virtual Appliance is listed under the ESXi host.
- 2 If it is listed, turn off the Security Virtual Appliance and delete it from the disk.
- 3 Revert the vShield Manager to the snapshot that you took before you tried to install the Security Virtual Appliance.
- 4 Reinstall the Security Virtual Appliance.

Once you have installed a Security Virtual Appliance, you can log in with the admin account.

Enabling Symantec Endpoint Protection clients to use a vShield-enabled Shared Insight Cache

To enable clients to use a vShield-enabled Shared Insight Cache

- 1 In the Symantec Endpoint Protection Manager console, open the appropriate Virus and Spyware Protection policy and click **Miscellaneous**.
- 2 On the **Miscellaneous** page, click **Shared Insight Cache**.
- 3 Check **Enable Shared Insight Cache**.
- 4 Click **Shared Insight Cache using VMware vShield**.
- 5 Click **OK**.

See [“What do I need to do to use a vShield-enabled Shared Insight Cache?”](#) on page 653.

Stopping and starting the vShield-enabled Shared Insight Cache service

Once you have installed a Security Virtual Appliance, the Shared Insight Cache service starts automatically. If you want to change the settings in the Shared Insight Cache configuration file, you should stop the service before you edit the file.

To stop the vShield-enabled Shared Insight Cache service

- 1 Log in to the Security Virtual Appliance as admin with the password that you assigned in the installation settings file.
- 2 On the command line, type the following command:

```
sudo stop vsic
```

To start the vShield-enabled Shared Insight Cache service

- 1 Log in to the Security Virtual Appliance as admin with the password that you assigned in the installation settings file.
- 2 On the command line, type the following command:

```
sudo start vsic
```

See [“Configuration file settings for a vShield-enabled Shared Insight Cache”](#) on page 666.

Service commands for the vShield-enabled Shared Insight Cache

To issue service commands, you must log on to the Security Virtual Appliance using the admin account. The default password is **symantec**, but you were prompted to change the password the first time that you logged in.

[Table 29-6](#) summarizes the commands that you can use.

Table 29-6 Service commands for the vShield-enabled Shared Insight Cache

Command	Description
<code>sudo start vsic</code>	Starts the vShield-enabled Shared Insight Cache service.
<code>sudo stop vsic</code>	Stops the vShield-enabled Shared Insight Cache service.
<code>sudo restart vsic</code>	If the vShield-enabled Shared Insight Cache service is running, stops the vShield-enabled Shared Insight Cache service and then starts it again.
<code>sudo status vsic</code>	Returns the status of the vShield-enabled Shared Insight Cache service.

See [“Configuration file settings for a vShield-enabled Shared Insight Cache”](#) on page 666.

See [“Stopping and starting the vShield-enabled Shared Insight Cache service”](#) on page 665.

Configuration file settings for a vShield-enabled Shared Insight Cache

The configuration file for a vShield-enabled Shared Insight Cache is an XML file that follows the .NET application configuration standard. The Shared Insight Cache service does not start if there is any invalid configuration, which includes invalid XML, incorrect value types, or missing required values.

The configuration file is named `SharedInsightCacheService.exe.config` and it is located in the `/etc/symantec` directory.

Note: Symantec has tested and optimized the default settings in this file for performance and scalability. Symantec recommends that you do not modify these settings. If you feel that you have a compelling reason to do so, we recommend that you contact Symantec Support first, before you make any changes.

Before you make any changes to the configuration file, create a backup copy of the file. You should also remember to restart the vShield-enabled Shared Insight Cache service after you have saved your changes.

Table 29-7 Configuration options

Option and default value	Description and comments
Cache prune size <code>prune.size="10"</code>	Percentage of memory usage to remove from the cache when the cache reaches the memory usage limit. The value must be between 10 and 100. If the value is not between 10 and 100, the server uses the default value of 10. Note: Avoid modifying this setting.
Cache memory usage <code>mem.usage="50"</code>	The maximum percentage of physical memory that the service is allowed to use. Once this value is reached, the service prunes the cache. This value must be 10 or greater.
Cache pruning interval <code>clean.interval="10"</code>	The interval in seconds at which the service checks to see if the cache should be pruned.
Enable performance statistics logging <code>enabled="true"</code>	Set to false to disable. Note: The <code>interval</code> attribute can override this setting.
Performance statistics log file <code>file="/data/Symantec/vSIC/vSIC_Perf.csv"</code>	The location of the file that collects performance data.
Performance statistics interval <code>interval="10"</code>	The interval, in seconds, at which statistics are recorded. If set to 0, this attribute disables recording and overrides the <code>enabled=true</code> attribute.
Performance statistics file maximum size <code>maxSize="1MB"</code>	The maximum size in bytes that the output file is allowed to reach before is rolled over to a backup file. You can also specify the maximum size in kilobytes, megabytes, or gigabytes. The value 10KB is interpreted as 10240 bytes.

Table 29-7 Configuration options (*continued*)

Option and default value	Description and comments
Number of performance statistics file backups <code>maxBackups="1"</code>	If set to zero, then there are no backup files and the log file is truncated when it reaches the maximum size (<code>maxSize</code> attribute). If this attribute is set to a negative number, then no deletions are made. Note: When you restart the service after you make a change to the <code>maxBackups</code> attribute, the existing backup files are overwritten. Symantec recommends that you move the existing backup files to a new location before you restart the service.

Table 29-8 Description of the logging configuration options

Option and default value	Description and comments
Log file <code>file value="/data/log/Symantec/vSIC.log"</code>	The file where the service logs information about the Security Virtual Appliance and vShield-enabled Shared Insight Cache.
Number of backup files to keep <code>maxSizeRollBackups value="1"</code>	If this attribute is set to zero, then there are no backup files and the log file is truncated when it reaches the value of the <code>maxSize</code> attribute. Note: When you restart the service after you make a change to the <code>maxBackups</code> attribute, the existing backup files are overwritten. Symantec recommends that you move the existing backup files to a new location before you restart the service.
Log size <code>maximumFileSize value="10MB"</code>	Size of the log (in bytes) before the oldest log is deleted.
Enable the local or remote logging option <code>appender-ref ref="LocalSyslogAppender"</code> <code>appender-ref ref="RemoteSyslogAppender"</code>	You can enable local or remote Syslog logging by uncommenting one of the options. Syslog is not enabled by default. If you want to log remotely, be sure to set the IP address for the <code>RemoteSyslogAppender</code> .
IP address for remote logging <code>remoteAddress value="192.168.x.y"</code>	You need to set this address if you enable remote logging.

Table 29-8 Description of the logging configuration options (*continued*)

Option and default value	Description and comments
Log level level value="ERROR"	ALL DEBUG INFO WARN ERROR FATAL OFF Each level includes the messages from the levels that are more critical as well. For example, ERROR logs the ERROR-level messages and the FATAL messages. The INFO level includes all messages except the debugging messages. Note: Set the value to OFF if you want to disable logging entirely.

See [“Stopping and starting the vShield-enabled Shared Insight Cache service”](#) on page 665.

For information about the .NET application configuration standard, see the following Web page:

[Configuration Editor Tool \(SvcConfigEditor.exe\)](#)

For more information about log4net configuration, see the following Web page:

[Apache Logging Services](#)

About vShield-enabled Shared Insight Cache event logging

Symantec Endpoint Protection logs the events from a Shared Insight Cache that is integrated with VMware vShield Endpoint to the `vSIC.log` file by default. This file is created in the `/data/log/Symantec` directory by default.

Logging is on by default and the level is set to `ERROR`. You can change the logging level and other logging attributes in the Shared Insight Cache configuration file.

See [“Configuration file settings for a vShield-enabled Shared Insight Cache”](#) on page 666.

Uninstalling a Symantec Endpoint Protection Security Virtual Appliance

You should use the command-line installation tool that Symantec supplies to uninstall a Security Virtual Appliance.

Note: Do not manually remove a Symantec Endpoint Protection Security Virtual Appliance. Use the Symantec Security Virtual Appliance installation tool to uninstall the Security Virtual Appliance. If you manually remove the Security Virtual Appliance, it does not unregister the Security Virtual Appliance from the VMware vShield Manager. This failure to unregister causes issues if you subsequently try to reinstall the Security Virtual Appliance.

To install or to uninstall the Security Virtual Appliance, the vCenter Administrator account that you use must have permissions in the following privilege categories:

- Datastore (All privileges)
- Network (All privileges)
- vApp (All privileges)
- Virtual Machine (All privileges)
- Global > Cancel Task

To uninstall Security Virtual Appliances

- 1 Navigate to the directory where you invoked the `Symantec_SVA_Install.jar` tool to install the Security Virtual Appliance.
- 2 Type the following command:

```
java -jar Symantec_SVA_Install.jar -s  
pathname/SVA_InstallSettings.xml -uninstall
```

Errors and other command output are written to the `SVA_Install.log` log file. This file is created in the same directory from which you executed the `Symantec_SVA_Install.jar` file command.

Note: In a few instances, the write to that directory may fail. In these cases, then the file is written to the `/temp` directory and is named `SVA_Installxxx.log`, where the system replaces `xxx` with a random number.

See [“About vShield-enabled Shared Insight Cache event logging”](#) on page 669.

Using Virtual Image Exception

This chapter includes the following topics:

- [Using the Virtual Image Exception tool on a base image](#)
- [System requirements for the Virtual Image Exception tool](#)
- [Running the Virtual Image Exception tool](#)
- [Configuring Symantec Endpoint Protection to bypass the scanning of base image files](#)

Using the Virtual Image Exception tool on a base image

You can use the Virtual Image Exception tool on a base image before you build out your virtual machines. The Virtual Image Exception tool lets your clients bypass the scanning of base image files for threats, which reduces the resource load on disk I/O. It also improves CPU scanning process performance in your virtual desktop infrastructure.

Symantec Endpoint Protection supports the use of the Virtual Image Exception tool for managed clients and unmanaged clients

Note: You cannot use the Virtual Image Exception tool in a non-virtual environment.

Table 30-1 Process for using the Virtual Image Exception tool on a base image

Step	Action
Step 1	<p>On the base image, perform a full scan all of the files to ensure that the files are clean.</p> <p>If the Symantec Endpoint Protection client quarantines infected files, you must repair or delete the quarantined files to remove them from quarantine.</p> <p>See "Specifying when repaired files, backup files, and quarantined files are automatically deleted" on page 447.</p>
Step 2	<p>Ensure that the client's quarantine is empty.</p> <p>See "Using the Risk log to delete quarantined files on your client computers" on page 449.</p>
Step 3	<p>Run the Virtual Image Exception tool from the command line to mark the base image files.</p> <p>See "Running the Virtual Image Exception tool" on page 673.</p> <p>See vietool on page 813.</p>
Step 4	<p>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.</p> <p>See "Configuring Symantec Endpoint Protection to bypass the scanning of base image files" on page 673.</p>
Step 5	<p>Remove the Virtual Image Exception tool from the base image.</p>

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 672.

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 and System Requirements for all versions of Symantec Endpoint Protection and Symantec Network Access Control](#)

See [“Using the Virtual Image Exception tool on a base image”](#) on page 671.

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 672.

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 813.

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 671.

Non-persistent virtual desktop infrastructures

This chapter includes the following topics:

- [Using Symantec Endpoint Protection in non-persistent virtual desktop infrastructures](#)
- [Setting up the base image for non-persistent guest virtual machines in VDIs](#)
- [Creating a registry key to mark the base image Guest Virtual Machines \(GVMs\) as non-persistent clients](#)
- [Configuring a separate purge interval for offline non-persistent VDI clients](#)

Using Symantec Endpoint Protection in non-persistent virtual desktop infrastructures

You can configure the Symantec Endpoint Protection client in your base image to indicate that it is a non-persistent virtual client. You can then configure a separate purge interval in Symantec Endpoint Protection for the offline guest virtual machines (GVMs) in non-persistent virtual desktop infrastructures. Symantec Endpoint Protection Manager removes the non-persistent GVM clients that have been offline longer than the specified time period. This feature makes it simpler to manage the GVMs in Symantec Endpoint Protection Manager.

Table 31-1 Tasks to use Symantec Endpoint Protection in non-persistent virtual desktop infrastructures

Step	Description
Step 1	Set up the base image. See “Setting up the base image for non-persistent guest virtual machines in VDIs” on page 676.
Step 2	In Symantec Endpoint Protection Manager, configure a separate purge interval for offline non-persistent VDI clients. See “Configuring a separate purge interval for offline non-persistent VDI clients” on page 678.

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 31-2 Tasks to set up the base image for non-persistent GVMs

Step	Description
Step 1	Install Symantec Endpoint Protection on the base image. See “About client installation methods” on page 115.
Step 2	In Symantec Endpoint Protection Manager, disable Tamper Protection so that you can modify the registry. See “Changing Tamper Protection settings” on page 494.
Step 3	Create a registry key on the base image to mark the GVMs as non-persistent clients. The advantage of non-persistent clients is that only online clients count toward the number of deployed licenses whereas offline non-persistent clients do not. See “Creating a registry key to mark the base image Guest Virtual Machines (GVMs) as non-persistent clients” on page 677.
Step 4	In Symantec Endpoint Protection Manager, enable Tamper Protection again. See “Changing Tamper Protection settings” on page 494.

After you have finished setting up the base image, you can configure a separate purge interval for non-persistent clients in Symantec Endpoint Protection Manager.

See [“Configuring a separate purge interval for offline non-persistent VDI clients”](#) on page 678.

See [“Using Symantec Endpoint Protection in non-persistent virtual desktop infrastructures”](#) on page 675.

Creating a registry key to mark the base image Guest Virtual Machines (GVMs) as non-persistent 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 create a registry key to mark the base image GVMs as non-persistent clients

- 1 After you have installed the Symantec Endpoint Protection client and disabled Tamper Protection, open the registry editor on the base image.
- 2 Navigate to 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 key named **Virtualization**.
- 4 Under **Virtualization**, create a key of type DWORD named **IsNPVDIClient** and set it to a value of 1.

See [“Setting up the base image for non-persistent guest virtual machines in VDIs”](#) on page 676.

Configuring a separate purge interval for offline non-persistent VDI clients

Over time, obsolete clients can accumulate in the Symantec Endpoint Protection Manager database. Obsolete clients are those clients that have not connected to Symantec Endpoint Protection Manager for 30 days. Symantec Endpoint Protection Manager purges obsolete clients every 30 days by default.

If you do not want to wait the same number of days to purge obsolete non-persistent clients, you can configure a separate interval for them. If you do not configure a separate interval, then offline non-persistent VDI clients are purged at the same interval that non-virtual obsolete clients are purged.

Note: Online non-persistent clients count toward the number of deployed licenses; offline non-persistent clients do not.

You can also filter the offline non-persistent clients out of the view on the **Clients** page.

To configure the purge interval for offline non-persistent VDI clients

- 1 In the Symantec Endpoint Protection Manager console, on the **Admin** page, click **Domains**.
- 2 In the **Domains** tree, click the desired domain.
- 3 Under **Tasks**, click **Edit Domain Properties**.
- 4 On the **Edit Domain Properties > General** tab, check the **Delete non-persistent VDI clients that have not connected for specified time** checkbox and change the **days** value to the desired number.

The **Delete clients that have not connected for specified time** option must be checked to access the option for offline non-persistent VDI clients.

- 5 Click **OK**.

See [“Using Symantec Endpoint Protection in non-persistent virtual desktop infrastructures”](#) on page 675.

Configuring and managing the management server

- [Chapter 32. Configuring the connection between the management server and the clients](#)
- [Chapter 33. Configuring the management server](#)
- [Chapter 34. Managing databases](#)
- [Chapter 35. Managing failover and load balancing](#)
- [Chapter 36. Managing sites and replication](#)
- [Chapter 37. Preparing for disaster recovery](#)

Configuring the connection between the management server and the clients

This chapter includes the following topics:

- [Setting up SSL communications between a Symantec Endpoint Protection Manager and the clients](#)
- [Improving client and server performance](#)
- [About server certificates](#)
- [Best practices for updating server certificates and maintaining the client-server connection](#)

Setting up SSL 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. The web server uses HTTP for all communications. HTTP is an unencrypted protocol and does not provide for the confidentiality or integrity of the communications over it. You can configure the Symantec Endpoint Protection Manager Apache web server to use a Secure Sockets Layer (SSL) certificate to sign and encrypt data using an HTTPS connection.

Table 32-1 Configuring SSL communication to the client

Step	Action	Description
1	Check that the default SSL port is available	By default, SSL traffic uses port 443. In some networks, port 443 may already be bound to another application or service. Before you enable SSL communication, you must check to see if the default port is available. See “Verifying port availability” on page 681.
2	Change the default SSL 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 Apache SSL port assignment for client communication” on page 682. See “Configuring a management server list for load balancing” on page 715.
3	Enable SSL communication to the client	Edit the Apache httpd.conf file to allow SSL communication to the client. Test the SSL connection, and then switch the clients to HTTPS communication. See “Enabling SSL for the Apache web server for client communication” on page 683.

See [“Managing the client-server connection”](#) on page 165.

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

- 1 Open a command prompt and execute the command:

```
netstat -an
```

- 2 In the Local Address column, look for an entry that ends with the port number you want to check.

For instance, to see if port 443 is available, look in the Local Address column for an entry that ends in 443. If no entry ends in 443, the port is available.

See [“Changing the Apache SSL port assignment for client communication”](#) on page 682.

See [“Setting up SSL communications between a Symantec Endpoint Protection Manager and the clients”](#) on page 680.

Changing the Apache SSL port assignment for client communication

You may be required to change the default SSL port assignment if the default SSL port is not available.

You must first verify that the new SSL port that you choose is unused. If you change the port assignment after you deploy managed clients, you must perform an additional task. This task ensures that the clients can continue to communicate with Symantec Endpoint Protection Manager.

After you complete these procedures, you enable SSL in Apache.

To change the Apache SSL port in the management server list

- 1 In the Symantec Endpoint Protection Manager console, on the **Policies** tab, click **Policy Components > Management Server Lists**.
- 2 Double-click on the management server list that your groups and locations use. If you only have the default management server list, duplicate the default management server list. Double-click the new list to edit it.
- 3 Under **Management Servers**, highlight the IP address entry for your management server, and then click **Add > New Priority**.
- 4 Click the priority you created and then click **Add > New Server**.
- 5 In the **Add Management Server** window, enter the server IP address, click **Customize HTTPS port**, enter the new port number, and then click **OK**.
- 6 Repeat steps 4 and 5, except use the computer name entry for your management server.
- 7 Click **OK**. If you did not edit a copy of the default management server list, go to step 9.
- 8 Right-click the copy of the default management server list and click **Assign**, then assign it to every group and location.
- 9 Verify that clients receive this updated policy before you begin the next procedure.

See [“Using the policy serial number to check client-server communication”](#) on page 172.

To change the Apache SSL port in the configuration file

- 1 In a text editor, open the following file:

```
%SEPM%\apache\conf\ssl\sslForClients.conf
```

Where %SEPM% is the Symantec Endpoint Protection Manager installation folder.

- 2 Edit the following strings 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 681.

See [“Enabling SSL for the Apache web server for client communication”](#) on page 683.

See [“Setting up SSL communications between a Symantec Endpoint Protection Manager and the clients”](#) on page 680.

Enabling SSL for the Apache web server for client communication

You edit the httpd.conf file to enable Secure Sockets Layer (SSL) communication between the Symantec Endpoint Protection Manager server and the clients.

If you need to use an alternate port for SSL communication, you must change the port assignment in Symantec Endpoint Protection Manager first.

To enable SSL for the Apache web server

- 1 In a text editor, open the following file:

```
%SEPM%\apache\conf\httpd.conf
```

Where %SEPM% is the Symantec Endpoint Protection Manager installation folder.

- 2 Find the following entry and remove the hash mark (#) from the text string:

```
#Include conf/ssl/sslForClients.conf
```

- 3 Save and then close the file.

- 4 Restart the **Symantec Endpoint Protection Manager Webserver** service.

See [“Stopping and starting the Apache Web server”](#) on page 749.

To verify SSL works correctly

- 1 Enter the following URL in a web browser:

```
https://ServerHostName:port/secars/secars.dll?hello,secars
```

Where *ServerHostName* is the computer name for Symantec Endpoint Protection Manager and *port* is the port number. By default, SSL traffic uses port 443.

- 2 If the browser displays the word "OK", the SSL 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.

To switch the clients to use SSL 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.

See ["Copying and pasting a policy on the Policies page"](#) on page 322.

- 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 688.

- 4 Click **OK**.
- 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 716.

As the clients receive the updated management server list, the clients switch to HTTPS for communication with Symantec Endpoint Protection Manager.

See ["Changing the Apache SSL port assignment for client communication"](#) on page 682.

See ["Setting up SSL communications between a Symantec Endpoint Protection Manager and the clients"](#) on page 680.

Improving client and server performance

Symantec Endpoint Protection Manager includes various features that enable you to increase the client performance and server performance while still maintaining a high level of security.

Table 32-2 Tasks to improve performance on the server and on the client

Task	Description
<p>Change client-server communication settings</p>	<p>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.</p> <p>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.</p> <p>See “Configuring push mode or pull mode to update client policies and content” on page 170.</p> <p>For more information about setting heartbeat intervals, see the Symantec Endpoint Sizing and Scalability Best Practices white paper.</p>
<p>Randomize and reduce the number of content updates</p>	<p>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:</p> <ul style="list-style-type: none"> ■ Distribute the client load across multiple management servers. See “Configuring a management server list for load balancing” on page 715. ■ 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 228. ■ Randomize the time when LiveUpdate downloads content to the client computers. See “Randomizing content downloads from a LiveUpdate server” on page 208. See “Randomizing content downloads from the default management server or a Group Update Provider” on page 207. ■ Download content updates when users are not actively using the client computer. See “Configuring client updates to run when client computers are idle” on page 209.

Table 32-2 Tasks to improve performance on the server and on the client
(continued)

Task	Description
Adjust scans to improve computer performance	<p>You can change some scan settings to improve the computers' performance without reducing protection.</p> <p>For example, you can configure scans to ignore trusted files or to run when the computer is idle.</p> <p>See "Adjusting scans to improve computer performance" on page 427.</p> <p>See "Customizing Auto-Protect for Windows clients" on page 464.</p>
Reduce database client log volume	<p>You can configure the logging options to optimize storage requirements and comply with company policies that control retention of logged data.</p> <p>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.</p> <p>You can reduce the volume of log data by performing the following tasks:</p> <ul style="list-style-type: none"> ■ 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 708. ■ Specify how many log entries the client computer can keep in the database, and how long to keep them. See "Specifying how long to keep log entries in the database" on page 709. ■ Filter the less important risk events and system events out so that less data is forwarded to the server. See "Modifying miscellaneous settings for Virus and Spyware Protection on Windows computers" on page 475. ■ Reduce the number of clients that each management server manages. See "Configuring a management server list for load balancing" on page 715. See "Installing Symantec Endpoint Protection Manager" on page 74. ■ Reduce the heartbeat frequency, which controls how often the client logs are uploaded to the server. See "Configuring push mode or pull mode to update client policies and content" on page 170. ■ 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 709.

Table 32-2 Tasks to improve performance on the server and on the client
(continued)

Task	Description
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 703.

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 688.

See [“Disabling or enabling secure communications between the server and the client”](#) on page 689.

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 735.

See [“Updating or restoring a server certificate”](#) on page 690.

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:

Symantec Endpoint Protection Manager installation folder\Server Private Key Backup\recovery_timestamp.zip

The password appears in the `keystore.password=` line.

- PKCS12 keystore file (.pfx and .p12)
- Certificate and private key file (.der and .pem format)
 Symantec supports unencrypted certificates and private keys in the .der or the .pem format. .Pkcs8-encrypted private keys are not supported.

Best practices for updating server certificates and maintaining the client-server connection

You may need to update the security certificate in the following situations:

- You restore a previous security certificate that the clients already use.
- You want to use a different security certificate than the default certificate (.jks).

When clients use secure communication with the server, the server certificate is exchanged between the server and the clients. This exchange establishes a trust relationship between the server and clients. When the certificate changes on the server, the trust relationship is broken and clients no longer can communicate. This problem is called orphaning clients.

Note: Use this process to update either one management server or multiple management servers at the same time.

[Table 32-3](#) lists the steps to update the certificate without orphaning the clients that the server manages.

Table 32-3 Steps to update server certificates

Step	Task	Description
1	Disable server certificate verification	Disable secure communications between the server and the clients. When you disable the verification, the clients stay connected while the server updates the server certificate. See “Disabling or enabling secure communications between the server and the client” on page 689.

Table 32-3 Steps to update server certificates (*continued*)

Step	Task	Description
2	Wait for all clients to receive the updated policy	<p>The process of deploying the updated policy may take a week or longer, depending on the following factors:</p> <ul style="list-style-type: none"> ■ 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. <p>See “Using the policy serial number to check client-server communication” on page 172.</p>
3	Update the server certificate	<p>Update the server certificate. If you migrate or upgrade the management server, upgrade the certificate first.</p> <p>See “Upgrading a management server” on page 152.</p> <p>See “Updating or restoring a server certificate” on page 690.</p>
4	Enable server certificate verification again	<p>Enable secure communications between the server and the clients again.</p> <p>See “Disabling or enabling secure communications between the server and the client” on page 689.</p>
5	Wait for all clients to receive the updated policy	<p>The client computers must receive the policy changes from the previous step.</p>
6	Restore replication relationship (optional)	<p>If the server you updated replicates with other management servers, restore the replication relationship.</p> <p>See “Turning on replication after an upgrade from Symantec Endpoint Protection 11.0” on page 155.</p>

Disabling or enabling secure communications between the server and the client

To authenticate communication between the management server and the client, the server uses a certificate. If the certificate is corrupted or invalid, the clients cannot communicate with the server. If you disable secure communications, then the clients can still communicate with the server. However, the clients do not authenticate communications from the management server.

You should temporarily disable secure communications between the clients and server for the following reasons:

- To move a large number of clients from one site to another site without needing to use the Sylink.xml file.

See [“Why do I need to replace the client-server communications file on the client computer?”](#) on page 173.

- To update a corrupted certificate or invalid certificate. You can update multiple management servers at the same time. As a best practice, you should perform disaster recovery instead.

See [“Updating or restoring a server certificate”](#) on page 690.

See [“Performing disaster recovery”](#) on page 737.

Make sure that you configure this setting for the groups that do not inherit from a parent group.

After you move the clients or update the certificate, you enable secure communications again.

Disabling or enabling secure communications between the server and the client

- 1 On the console, click **Clients > Policies > General Settings**.
- 2 On the **Security Settings** tab, check or uncheck **Enable secure communications between the management server and clients by using digital certificates for authentication**.
- 3 Click **OK**.

See [“About server certificates”](#) on page 687.

See [“Best practices for updating server certificates and maintaining the client-server connection”](#) on page 688.

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 74.
- 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 687.
- You upgraded from a legacy 11.0 management server.
See [“Upgrading a management server”](#) on page 152.

See [“Best practices for updating server certificates and maintaining the client-server connection”](#) on page 688.

To update or restore a server certificate

- 1 In the console, click **Admin**, and then click **Servers**.
- 2 Under **Servers**, under **Local Site**, click the management server for which you want to update the server certificate.
- 3 Under **Tasks**, click **Manage Server Certificate**, and then click **Next**.
- 4 In the **Manage Server Certificate** panel, click **Update the server certificate**, click **Next**, and then click **Yes**.

To maintain the server-client connection, disable secure connections.

See [“Disabling or enabling secure communications between the server and the client”](#) on page 689.

- 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 *Symantec Endpoint Protection Manager installation folder*\Server Private Key Backup\recovery_timestamp.zip. You can locate the password for the keystore file in the `settings.properties` file within the same .zip file. The password appears in the `keystore.password=` line.

- 7 You must log off and restart the management server for the certificate to become effective.

See [“Stopping and starting the management server service”](#) on page 156.

Configuring the management server

This chapter includes the following topics:

- [Managing Symantec Endpoint Protection Manager servers and third-party servers](#)
- [About the types of Symantec Endpoint Protection servers](#)
- [Exporting and importing server settings](#)
- [Enabling or disabling Symantec Endpoint Protection Manager web services](#)

Managing Symantec Endpoint Protection Manager servers and third-party servers

You can configure Symantec Endpoint Protection Manager to integrate with many of the different types of servers in your network environment.

Table 33-1 Server management

Task	Description
Learn about servers	Decide which types of servers you need to set up. See “About the types of Symantec Endpoint Protection servers” on page 695.

Managing Symantec Endpoint Protection Manager servers and third-party servers

Table 33-1 Server management (*continued*)

Task	Description
Set server communication permissions	<p>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.</p> <p>See “Granting or blocking access to remote Symantec Endpoint Protection Manager consoles” on page 83.</p>
Modify server settings	<p>To modify database settings, or to restore your database on a different computer, you can modify server settings.</p> <p>See “Reinstalling or reconfiguring Symantec Endpoint Protection Manager” on page 738.</p>
Configure the mail server	<p>To work with a specific mail server in your network, you need to configure the mail server.</p> <p>See “Establishing communication between the management server and email servers” on page 628.</p>
Manage directory servers	<p>You can integrate Symantec Endpoint Protection with directory servers to help manage administrator accounts or to create organizational units.</p> <p>See “Connecting Symantec Endpoint Protection Manager to a directory server” on page 242.</p>
Configure proxy settings if you use a proxy server to connect to Symantec LiveUpdate servers	<p>To set up the Symantec Endpoint Protection Manager to connect to the Internet through a proxy server, you must configure the proxy server connection.</p> <p>See “Configuring Symantec Endpoint Protection Manager to connect to a proxy server to access the Internet and download content from Symantec LiveUpdate” on page 195.</p>
Import or export server properties	<p>You can export server settings to an xml file, and you can re-import the same settings.</p> <p>See “Exporting and importing server settings” on page 695.</p>

Table 33-1 Server management (*continued*)

Task	Description
Manage server certificates	<p>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.</p> <p>See “About server certificates” on page 687.</p> <p>See “Updating or restoring a server certificate” on page 690.</p> <p>See “Backing up a server certificate” on page 735.</p> <p>See “Generating a new server certificate” on page 740.</p>
Configure SecurID Authentication for a server	<p>If you choose to authenticate administrator accounts by using RSA SecurID, you must also configure the management server to communicate with the RSA server.</p> <p>See “Configuring the management server to authenticate administrators who use RSA SecurID to log on” on page 298.</p>
Move the server to a different computer	<p>You may need to move the management server software from one computer to another for the following reasons:</p> <ul style="list-style-type: none"> ■ 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. <p>You can move the management server software in the following ways:</p> <ul style="list-style-type: none"> ■ Install the management server on another computer and perform replication. See “Re-adding a replication partner that you previously deleted” on page 730. ■ Install the management server on another computer using the recovery file. See “Reinstalling or reconfiguring Symantec Endpoint Protection Manager” on page 738.
Start and stop the management server	<p>The management server runs as an automatic service. You must stop the management server service when you upgrade, or perform disaster recovery.</p> <p>See “Stopping and starting the management server service” on page 156.</p>

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 718.
- **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 712.
- **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 698.
- **Replication partner**
A relationship created between two sites to enable data replication between them.
See [“Setting up sites and replication”](#) on page 718.

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 692.

To export server settings

- 1 In the console, click **Admin**, and then click **Servers**.
- 2 Under **Servers**, expand **Local Site (Site *site_name*)**, and then select the management server you want to export.
- 3 Click **Export Server Properties**.
- 4 Select a location in which to save the file and specify a file name.
- 5 Click **Export**.

To import server settings

- 1 In the console, click **Admin**, and then click **Servers**.
- 2 Under **Servers**, expand **Local Site (Site *site_name*)**, and then select the management server for which you want to import settings.
- 3 Click **Import Server Properties**.
- 4 Select the file you want to import, and then click **Import**.
- 5 Click **Yes**.

Enabling or disabling Symantec Endpoint Protection Manager web services

Symantec Endpoint Protection provides two sets of web services on the management server. One set was written to provide integration with Symantec Protection Center. The other set was written to provide support for development of remote management applications.

The web services that Symantec Endpoint Protection Manager provides for remote management are enabled by default. You can disable them if you need to block the port, or if you need to reassign the port for a different service.

In 12.1.6, the web services for Protection Center are disabled by default.

To enable or disable Symantec Endpoint Protection Manager web services

- 1 In a command window, run the following batch file:

Symantec_Endpoint_Protection_Manager_installation_folder/ToolsConfigSEPM.bat

- 2 Set either of the following options:

-RmmWS:ON	Enables web services for remote management.
-RmmWS:OFF	Disables web services for remote management.
-SpCWS:ON	Enables web services for the Symantec Protection Center.
-SpCWS:OFF	Disables web services for the Symantec Protection Center.

Managing databases

This chapter includes the following topics:

- [Maintaining the database](#)
- [Scheduling automatic database backups](#)
- [Scheduling automatic database maintenance tasks](#)
- [Exporting data to a Syslog server](#)
- [Exporting log data to a text file](#)
- [Exporting log data to a comma-delimited text file](#)
- [Specifying client log size and which logs to upload to the management server](#)
- [Specifying how long to keep log entries in the database](#)
- [About increasing the disk space on the server for client log data](#)
- [Clearing log data from the database manually](#)

Maintaining the database

Symantec Endpoint Protection supports both an embedded database and the Microsoft SQL Server database. If you have more than 5,000 clients, you should use a Microsoft SQL Server database.

Symantec Endpoint Protection Manager automatically installs an embedded database. The database contains information about security policies, configuration settings, attack data, logs, and reports.

After you install Symantec Endpoint Protection Manager, the management server may start to slow down after a few weeks or a few months. To improve the

management server performance, you may need to reduce the database storage space and schedule various database maintenance tasks.

Table 34-1 Database management tasks

Task	Description
Schedule regular database backups	<p>You should schedule regular database backups in case the database gets corrupted.</p> <p>See “Backing up the database and logs” on page 733.</p> <p>See “Scheduling automatic database backups” on page 702.</p> <p>See “Performing disaster recovery” on page 737.</p> <p>Optionally, to prevent an automatic sweep of the database until after a backup occurs, you can manually sweep data from the database.</p> <p>See “Clearing log data from the database manually” on page 710.</p>
Schedule database maintenance tasks	<p>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.</p> <ul style="list-style-type: none"> ■ Remove unused data from the transaction log. ■ Rebuild the database table indexes to improve the database's sorting and searching capabilities. <p>See “Scheduling automatic database maintenance tasks” on page 703.</p>
Periodically check the database file size	<p>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.</p> <p>See “Increasing the Microsoft SQL Server database file size” on page 704.</p>

Table 34-1 Database management tasks (*continued*)

Task	Description
Calculate the database storage space that you need	<p>Before you can decide how to reduce the amount of storage space, calculate the total amount of disk space that you need.</p> <p>The database storage is based on the following factors:</p> <ul style="list-style-type: none"> ■ Log size and expiration time period. ■ The number of client computers. ■ The average number of viruses per month. ■ The number of events you need to retain for each log. ■ The number of content updates. The content updates require about 300 MB each. See “Configuring a site to download content updates” on page 189. See “Configuring the content revisions that clients use” on page 205. ■ 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. <p>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.</p>

Table 34-1 Database management tasks (*continued*)

Task	Description
Reduce the volume of log data	<p>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.</p> <p>You can reduce the volume of log data by performing the following tasks:</p> <ul style="list-style-type: none"> ■ 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 708. ■ Specify how many log entries the client computer can keep in the database, and how long to keep them. See “Specifying how long to keep log entries in the database” on page 709. ■ Filter the less important risk events and system events out so that less data is forwarded to the server. See “Modifying miscellaneous settings for Virus and Spyware Protection on Windows computers” on page 475. ■ 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 709. ■ Reduce the number of clients that each management server manages. See “Configuring a management server list for load balancing” on page 715. ■ Reduce the heartbeat frequency, which controls how often the client logs are uploaded to the server. See “Configuring push mode or pull mode to update client policies and content” on page 170.
Export log data to another server	<p>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.</p> <p>See “Exporting log data to a text file” on page 706.</p> <p>See “Exporting data to a Syslog server” on page 705.</p>
Create client installation packages with only the protection that you need	<p>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.</p> <p>See “Configuring Windows client installation feature sets” on page 127.</p>

Table 34-1 Database management tasks (*continued*)

Task	Description
Use the Group Update Provider to download content	<p>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.</p> <p>See “Using Group Update Providers to distribute content to clients” on page 215.</p> <p>To reduce disk space and database size, you can reduce the number of content revisions that are kept on the server.</p> <p>See “Configuring a site to download content updates” on page 189.</p>
Restore the database	<p>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.</p> <p>See “Restoring the database” on page 740.</p>

See [“Verifying the connection with the database”](#) on page 755.

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 733.

To schedule automatic database backups

- 1 In the console, click **Admin**, and then click **Servers**.
- 2 Under **Servers**, click the icon that represents the database that you want to back up.
- 3 Under **Tasks**, click **Edit Database Properties**.
- 4 In the **Database Properties** dialog box, on the **Backup Settings** tab, do the following tasks.
 - In the **Backup server** drop-down list, specify on which management server you want to save the backup.

- Check **Back up logs** if you need to save a copy of the logs for security purposes or company policy.
Otherwise, leave this option disabled, as logs use a lot of disk space.
 - Specify the number of backups if your company policy requires it.
- 5 Make sure **Schedule Backups** is checked, and set the schedule.
 - 6 Click **OK**.

Scheduling automatic database maintenance tasks

After you install the management server, the space in the database grows continually. The management server slows down after a few weeks or months. To reduce the database size and to improve the response time with the database, the management server performs the following database maintenance tasks:

- Truncates the transaction log.
The transaction log records almost every change that takes place within the database. The management server removes unused data from the transaction log.
- Rebuilds the index.
The management server defragments the database table indexes to improve the time it takes to sort and search the database.

By default, the management server performs these tasks on a schedule. You can perform the maintenance tasks immediately, or adjust the schedule so that it occurs when users are not on their computers.

Note: You can also perform the database maintenance tasks in Microsoft SQL Server Management Studio. However, you should perform these tasks in either Symantec Endpoint Protection Manager or Management Studio, but not both. See the knowledge base article: [Create database maintenance plans in MS SQL Server 2005 using SQL Server Integration Services \(SSIS\)](#).

To run database maintenance tasks on demand

- 1 In the console, click **Admin**, and then click **Servers**.
- 2 Under **Servers**, click the icon that represents the database.
- 3 Under **Tasks**, select either of the following options:
 - **Truncate Transaction Log Now**
 - **Rebuild Indexes Now**

- 4 Click **Run**.
- 5 After the task completes, click **Close**.

To schedule database maintenance tasks to run automatically

- 1 In the console, click **Admin**, and then click **Servers**.
- 2 Under **Servers**, click the icon that represents the database.
- 3 Under **Tasks**, click **Edit Database Properties**.
- 4 On the **General** tab, check either or both of the following options, then click **Schedule Task** and specify the schedule for each task.
 - **Truncate the database transaction logs**. The default schedule for this task is every four hours.
 - **Rebuild Indexes**. The default schedule for this task is every Sunday at 2:00.

Warning: If you perform these tasks in SQL Server Management Studio, uncheck these options.

See [“Scheduling automatic database backups”](#) on page 702.

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 703.

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 706.

To export log data to a Syslog server

- 1 In the console, click **Admin**.
- 2 Click **Servers**.
- 3 Click the local site or remote site that you want to export log data from.
- 4 Click **Configure External Logging**.
- 5 On the **General** tab, in the **Update Frequency** list box, select how often to send the log data to the file.
- 6 In the **Master Logging Server** list box, select the management server to send the logs to.

If you use SQL Server and connect multiple management servers to the database, specify only one server as the Master Logging Server.

- 7 Check **Enable Transmission of Logs to a Syslog Server**.
- 8 Provide the following information:
 - **Syslog Server**
Type the IP address or domain name of the Syslog server that you want to receive the log data.
 - **Destination Port**
Select the protocol to use, and type the destination port that the Syslog server uses to listen for Syslog messages.
 - **Log Facility**
Type the number of the log facility that you want to the Syslog configuration file to use, or use the default. Valid values range from 0 to 23.
- 9 On the **Log Filter** tab, check which logs to export.
- 10 Click **OK**.

Exporting log data to a text file

When you export data from the logs to a text file, by default the files are placed in a folder. That folder path is *Symantec Endpoint Protection Manager installation folder\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 34-2](#) shows the correspondence of the types of log data to the names of the exported log data files. The log names do not correspond one-to-one to the log names that are used on the **Logs** tab of the **Monitors** page.

Table 34-2 Log text file names for Symantec Endpoint Protection

Log Data	Text File Name
Server Administration	scm_admin.log
Application and Device Control	agt_behavior.log
Server Client	scm_agent_act.log
Server Policy	scm_policy.log
Server System	scm_system.log
Client Packet	agt_packet.log
Client Proactive Threat	agt_proactive.log
Client Risk	agt_risk.log
Client Scan	agt_scan.log
Client Security	agt_security.log
Client System	agt_system.log
Client Traffic	agt_traffic.log

Note: When you export to a text file, the number of exported records can differ from the number that you set in the **External Logging** dialog box. This situation arises when you restart the management server. After you restart the management server, the log entry count resets to zero, but there may already be entries in the temporary log files. In this situation, the first *.log file of each type that is generated after the restart contains more entries than the specified value. Any log files that are subsequently exported contain the correct number of entries.

To export log data to a text file

- 1 In the console, click **Admin**.
- 2 Click **Servers**.
- 3 Click the local site or remote site that you want to configure external logging for.
- 4 Click **Configure External Logging**.
- 5 On the **General** tab, select how often you want the log data to be sent to the file.
- 6 In the **Master Logging Server** list box, select the server that you want to send logs to.

If you use Microsoft SQL with more than one management server connecting to the database, only one server needs to be a Master Logging Server.
- 7 Check **Export Logs to a Dump File**.
- 8 If necessary, check **Limit Dump File Records** and type in the number of entries that you want to send at a time to the text file.
- 9 On the **Log Filter** tab, select all of the logs that you want to send to text files.

If a log type that you select lets you select the severity level, you must check the severity levels that you want to export.
- 10 Click **OK**.

Exporting log data to a comma-delimited text file

You can export the data in the logs to a comma-delimited text file.

See [“Exporting data to a Syslog server”](#) on page 705.

To export logs to a comma-delimited text file

- 1 In the console, click **Monitors**.
- 2 On the **Logs** tab, select the log that you want to export.

- 3 Click **View Log**.
- 4 Click **Export**.
- 5 In **File Download** dialog box, click **Save**.
- 6 Specify the file name and location, and then click **Save**.
- 7 Click **Close**.

Specifying client log size and which logs to upload to the management server

Company policy might require you to increase the time and type of log events that the database keeps. You can specify the number of entries kept in the logs and the number of days that each entry is kept on the client.

You can configure whether to upload each type of client log to the server. You can also configure the maximum size of the uploads. 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 how long to keep log entries in the database”](#) on page 709.

To specify client log size and which logs to upload to the management server

- 1 On the console, click **Clients**, and select a group.
- 2 On the **Policies** tab, under **Location-independent Policies and Settings**, click **Client Log Settings**.
- 3 In the **Client Log Settings** for *group name* dialog box, set the maximum file size and the number of days to keep log entries.
- 4 Check **Upload to management server** for any logs that you want the clients to forward to the server.

- 5 For the **Security** log and **Traffic** log, set the damper period and the damper idle period.

These settings determine how frequently **Network Threat Protection** events are aggregated.
- 6 Click **OK**.

Specifying how long to keep log entries in the database

To help control hard disk space, you can decrease the number of log entries that the database keeps. You can also configure the number of days the entries are kept.

Note: Log information on the Symantec Endpoint Protection Manager console **Logs** tab on the **Monitors** page is presented in logical groups for you to view. The log names on the **Site Properties Log Settings** tab correspond to log content rather than to log types on the **Monitors** page **Logs** tab.

See [“Specifying client log size and which logs to upload to the management server”](#) on page 708.

To specify how long to keep log entries in the database

- 1 In the console, click **Admin**.
- 2 Under **Servers**, expand **Local Site**, and click the database.
- 3 Under **Tasks**, click **Edit Database Properties**.
- 4 On the **Log Settings** tab, set the number of entries and number of days to keep log entries for each type of log.
- 5 Click **OK**.

About increasing the disk space on the server for client log data

A configuration that uploads a large volume of client log data to the server at frequent intervals can cause disk space problems on the server. If you must upload a large volume of client log data, you may have to adjust some default values to avoid these space problems. As you deploy to clients, you should monitor the space on the server in the log insertion directory and adjust these values as needed.

The default directory where the logs are converted to .dat files and then written to the database is in the following location:

Symantec Endpoint Protection Manager installation folder\data\inbox\log.

To adjust the values that control the space available on the server, you must change these values in the Windows registry. The Windows registry keys that you need to change are located on the server in HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\SEPM.

[Table 34-3](#) lists the Windows registry keys and their default values and describes what they do.

Table 34-3 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 698.

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 733.

See [“Specifying how long to keep log entries in the database”](#) on page 709.

To clear log data from the database manually

- 1 To prevent an automatic sweep of the database until after a backup occurs, increase a site's log size to their maximums.
- 2 Perform the backup, as appropriate.
- 3 On the computer where the manager is installed, open a Web browser and type the following URL:

`https://localhost:8443/servlet/ConsoleServlet?ActionType=ConfigServer&action=SweepLogs`

After you have performed this task, the log entries for all types of logs are saved in the alternate database table. The original table is kept until the next sweep is initiated.

- 4 To empty all but the most current entries, perform a second sweep. The original table is cleared and entries then start to be stored there again.
- 5 Return the settings on the **Log Settings** tab of the **Site Properties** dialog box to your preferred settings.

Managing failover and load balancing

This chapter includes the following topics:

- [Setting up failover and load balancing](#)
- [About failover and load balancing](#)
- [Configuring a management server list for load balancing](#)
- [Assigning a management server list to a group and location](#)

Setting up failover and load balancing

The client computers must be able to connect to a management server at all times to download the security policy and to receive log events.

Failover is used to maintain communication with a Symantec Endpoint Protection Manager when the management server becomes unavailable. Load balancing is used to distribute client management between multiple management servers 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 35-1](#) lists the tasks that you should perform to set up failover and load balancing.

Table 35-1 Process for setting up failover and load balancing

Tasks	Description
Read about failover and load balancing.	<p>You should understand if and when you need to set up management servers for failover and load balancing.</p> <p>See “About failover and load balancing” on page 713.</p>
Install additional management servers.	<p>Installing a Symantec Endpoint Protection Manager server for failover or load balancing</p> <p>The number of clients for each management server depends on several factors, such as the log sizes.</p> <p>To calculate how many management servers you need, see: Symantec Endpoint Protection Sizing and Scalability Best Practices White Paper</p>
Add management servers to a management server list.	<p>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.</p> <p>See “Configuring a management server list for load balancing” on page 715.</p>
Assign the custom management server list to a group.	<p>After you have created a custom management server list, you must assign the management server list to a group.</p> <p>See “Assigning a management server list to a group and location” on page 716.</p>

See [“Setting up sites and replication”](#) on page 718.

If the management server goes offline, or the client and the management server do not communicate, you should also troubleshoot the problem.

See [“Troubleshooting communication problems between the management server and the client”](#) on page 745.

About failover and load balancing

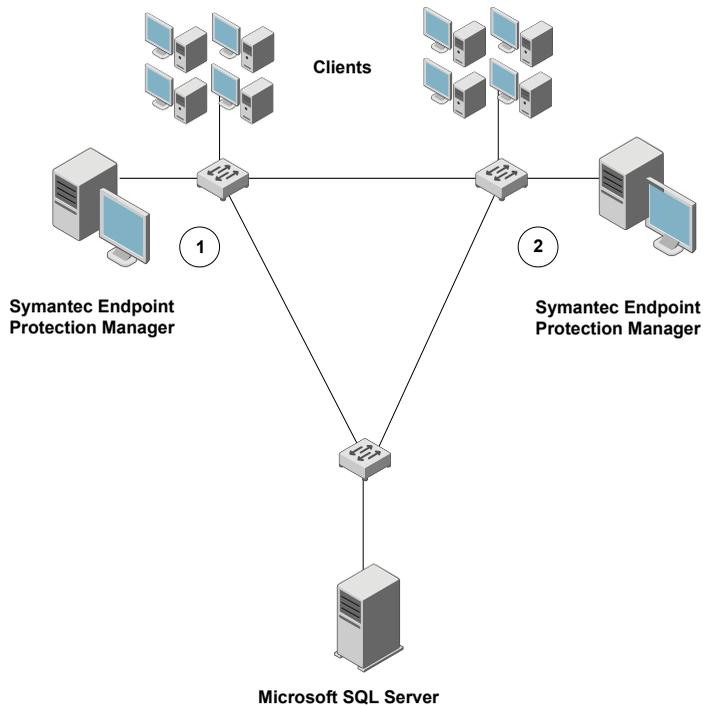
You can install two or more management servers that communicate with one Microsoft SQL Server database and configure them for failover or load balancing. Since you can install only one Symantec Endpoint Protection Manager to communicate with the embedded database, you can set up failover only if you

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 35-1 shows components on different subnets. Management servers and database servers can be on the same subnets. The servers are identified with the numbers 1 and 2, which signify a failover configuration.

Figure 35-1 Failover configuration



In a failover configuration, all clients send traffic to and receive traffic from server 1. If server 1 goes offline, all clients send traffic to and receive traffic from server 2 until server 1 comes back online. The database is illustrated as a remote installation, but it also can be installed on a computer that runs the Symantec Endpoint Protection Manager.

You may also want to consider failover for content updates, if you intend to use local servers. All the components that run LiveUpdate can also use a prioritized list of update sources. Your management servers can use a local LiveUpdate server and failover to LiveUpdate servers in other physical locations.

Note: The use of internal LiveUpdate servers, Group Update Providers, and site replication does not provide load balancing functionality. You should not set up multiple sites for load balancing.

See [“Setting up failover and load balancing”](#) on page 712.

See [“Configuring a management server list for load balancing”](#) on page 715.

See [“About determining how many sites you need”](#) on page 722.

See [“Setting up sites and replication”](#) on page 718.

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 713.

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 716.

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 715.

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**.

Managing sites and replication

This chapter includes the following topics:

- [Setting up sites and replication](#)
- [Deciding whether or not to set up multiple sites and replication](#)
- [About determining how many sites you need](#)
- [How replication works](#)
- [Replicating data without a schedule](#)
- [Replicating data on a schedule](#)
- [Specifying which data to replicate](#)
- [Deleting replication partners](#)
- [Re-adding a replication partner that you previously deleted](#)

Setting up sites and replication

A site consists of one database, one or more management servers, and clients. By default, you deploy Symantec Endpoint Protection as a single site. Organizations with more than one datacenter or physical location generally use multiple sites.

[Table 36-1](#) displays the steps to follow to set up additional sites and replication.

Table 36-1 Process for setting up sites

Steps	Tasks	Description
Step 1	Determine whether you need to add another site.	<p>Before you set up multiple sites and replication, make sure that it is necessary. Symantec recommends that you set up replication only in specific circumstances. If you do add an additional site, decide which site design works for your organization.</p> <p>For more information on whether or not to set up replication, see the following knowledge base article: When to use replication with Symantec Endpoint Protection Manager</p> <p>See “Deciding whether or not to set up multiple sites and replication” on page 720.</p> <p>See “About determining how many sites you need” on page 722.</p> <p>See “How replication works” on page 724.</p>
Step 2	Install Symantec Endpoint Protection Manager on the first site.	<p>When you install Symantec Endpoint Protection for the first time, by default you have installed the first site, or the local site.</p> <p>See “Installing Symantec Endpoint Protection Manager” on page 74.</p>
Step 3	Install Symantec Endpoint Protection Manager on the second site.	<p>You install the management server for the second site by using the Management Server Configuration wizard. In the wizard, click the Install an additional site option and following the instructions in the wizard.</p> <p>The second management server is classified as a remote site and called a replication partner.</p> <p>When you add the second site as a replication partner, you perform the following tasks:</p> <ul style="list-style-type: none"> ■ By default, replication is scheduled to occur automatically. However, you can change the replication schedule, based on the amount of disk space that is available. See “Replicating data on a schedule” on page 728. ■ Choose whether to replicate logs, client installation packages, or LiveUpdate content. See “Specifying which data to replicate” on page 729. <p>Symantec recommends that you add a maximum of five sites in the site farm.</p> <p>For information on how to set up replication, see the following video: Replication Concepts and Configuration</p>

Table 36-1 Process for setting up sites (*continued*)

Steps	Tasks	Description
Step 4	Replicate the data between the two sites.	<p>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.</p> <p>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.</p> <p>See “Replicating data without a schedule” on page 727.</p> <p>See “Replicating data on a schedule” on page 728.</p>

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 733.

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 738.

If you delete a replication partner to migrate or upgrade to the latest version of the management server, you must re-add the replication partner.

See [“Deleting replication partners”](#) on page 729.

See [“Re-adding a replication partner that you previously deleted”](#) on page 730.

See [“Connecting to a directory server on a replicated site”](#) on page 243.

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.

Deciding whether or not to set up multiple sites and replication

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 36-2](#) helps you decide whether to use more than one site with replication, to use a GUP, or to use neither.

Table 36-2 Deciding whether you need additional sites

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. <ul style="list-style-type: none"> ■ For a slow WAN link, consider using replication. ■ For multiple locations, consider using a GUP.
	No. Do you have a slow WAN link that connects to a location with more than 1,000 clients?	No. You do not need either replication or a GUP.
		Yes. Consider using replication.
		No. You do not need either replication or a GUP.

Table 36-2 Deciding whether you need additional sites (*continued*)

Question	Answer	Use multiple sites with replication or use a GUP
Do you have a slow WAN link?	Yes.	Yes. Consider using replication.
	Do you have multiple locations with more than 1,000 clients per location?	No. Consider using a GUP.
	No.	Yes. Consider using replication.
	Do you have multiple locations with more than 1,000 clients per location?	No. You do not need either replication or a GUP.
Do you have multiple locations with more than 1,000 clients per location?	Yes.	Yes. Consider using a GUP.
	Do you have a slow WAN link that connects to a location with more than 1,000 clients?	No. You do not need either replication or a GUP.
	No	Yes. Consider using a GUP.
	Do you have a slow WAN link that connects to a location with more than 1,000 clients?	No. You do not need either replication or a GUP.

See [“Using Group Update Providers to distribute content to clients”](#) on page 215.

See [“Setting up sites and replication”](#) on page 718.

See [“About determining how many sites you need”](#) on page 722.

About determining how many sites you need

A majority of small and medium-sized organizations need only a single site to centrally manage network security. Since each site has only one database, all data is centrally located.

Even a large organization with a single geographic location typically needs only needs one site. But for the organizations that are too complex to manage centrally, you should use a distributed management architecture with multiple sites.

You should consider multiple sites for any of the following factors:

- A large number of clients.
- The number of geographical locations and the type of communications links between them.
- The number of functional divisions or administrative groups.

- The number of datacenters. A best practice is to set up one Symantec Endpoint Protection site for each datacenter.
- How frequently you want to update the content.
- How much client log data you need to retain, how long you need to retain it, and where it should be stored.
- A slow WAN link between multiple physical locations with thousands of clients. If you set up a second site with its own management server, you can minimize the client-server traffic over that slow link. With fewer clients, you should use a Group Update Provider. See [“Using Group Update Providers to distribute content to clients”](#) on page 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 45,000 to 50,000 clients to a management server.

After you add a site, you should duplicate site information across multiple sites by replication. Replication is the process of sharing information between databases to ensure that the content is consistent.

[Table 36-3](#) displays the multi-site designs you can choose from.

Table 36-3 Multi-site designs

Site design	Description
Distributed	Each site performs replication bi-directionally for groups and policies, but not logs and content. To view the site reports, you use the console to connect to a management server in the remote site. Use this design when you do not need immediate access to remote site data.
Centralized logging	All logs are forwarded from the other sites to a central site. Use this design when you require centralized reporting.

Table 36-3 Multi-site designs (*continued*)

Site design	Description
High availability	<p>Each site has multiple management server installations and database clustering.</p> <p>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.</p> <p>You use this design to provide redundancy, failover, and disaster recovery.</p> <p>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.</p> <p>See “Setting up failover and load balancing” on page 712.</p>

For more information on whether or not to set up replication, see the following knowledge base article: [When to use replication with Symantec Endpoint Protection Manager](#)

See [“How replication works”](#) on page 724.

See [“Setting up sites and replication”](#) on page 718.

See [“Deciding whether or not to set up multiple sites and replication”](#) on page 720.

How replication works

Replication enables data to be duplicated between databases on separate sites so that both databases contain the same information. If one database fails, you can manage each site by using the information on the database from the second site.

A partner is a management server on another site with a different management server and database. A site may have as many partners as needed. Each partner, or remote site, connects to the main site or local site, which is the site that you are logged on to. All sites that are set up as partners are considered to be in the same site farm.

Each site you replicate data with is either a replication partner or a site partner. Both replication partners and site partners use multiple management servers, but the database they use and the way in which they communicate is different:

- Replication partners can use either an embedded database or a Microsoft SQL Server database. The management servers do not share the database. All replication partners share a common license key.

If you use an embedded database, you can only connect one Symantec Endpoint Protection Manager. If you use the Microsoft SQL Server database, you can connect multiple management servers that share one database. Only one of the management servers needs to be set up as a replication partner.

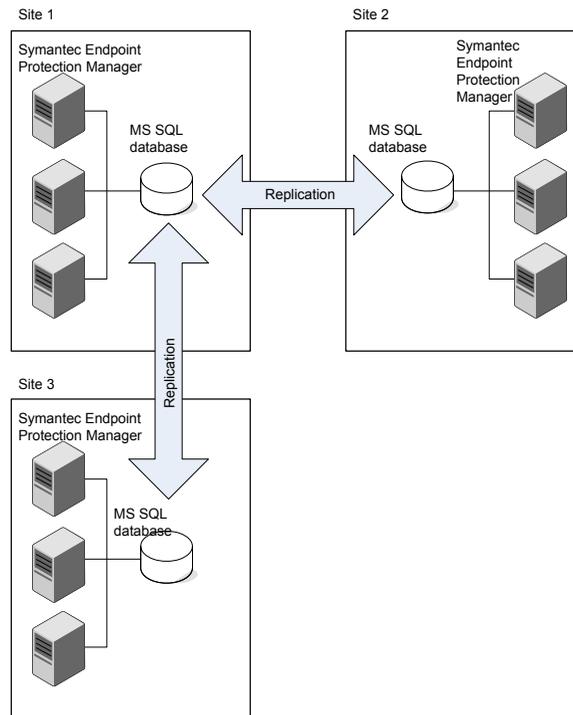
- Site partners share a single Microsoft SQL Server database.

The changes that you make on any partner are duplicated to all other partners. For example, you may want to set up one site at your main office (site 1) and a second site (site 2). Site 2 is a partner to site 1. The databases on site 1 and site 2 are reconciled by using the replication schedule. If a change is made on site 1, it automatically appears on site 2 after replication occurs. If a change is made on site 2, it automatically appears on site 1 after replication occurs. You can also install a third site (site 3) that can replicate data from either site 1 or site 2.

After replication occurs, the database on site 1 and the database on site 2 are the same. Only computer identification information for the servers differs.

Groups and policies are always replicated. You can choose to replicate logs, updated content, and patches.

Figure 36-1 How replication works between the main site and two remote sites



See [“How to resolve data conflicts between sites during replication”](#) on page 726.

See [“Specifying which data to replicate”](#) on page 729.

See [“About determining how many sites you need”](#) on page 722.

For more information on how often to replicate, see the following knowledge base article: [The Philosophy of SEPM Replication Setup](#)

See [“Setting up sites and replication”](#) on page 718.

How to resolve data conflicts between sites during replication

If administrators change settings on the sites in a site farm, conflicts can occur.

[Table 36-4](#) displays the ways that Symantec Endpoint Protection Manager handles the conflicts that arise.

Table 36-4 How the management server resolves conflicts between sites

Conflict type	Example	Resolution
Two differences cannot exist together.	Administrators for site 1 and site 2 both configure an identical Firewall policy setting. On site 1, the setting is enabled. On site 2, the setting is disabled.	The management server retains only the most recently made change. For example, if you made a change on site 1 first, and site 2 second, then the site 2 change is retained.
The same variable is created for both sites.	Administrators on site 1 and site 2 both add a group with the same name.	The management server retains both changes, adding a tilde and the numeral 1 (~1) after the more recently made variable. For example, with two groups named as Sales, the most recently named Sales group becomes Sales ~1.
Data can merge without conflict.	The administrator for site 1 adds two Firewall policies and the administrator for site 2 adds five Firewall policies.	The management server merges the changes For example, the management server displays all seven Firewall policies on both sites.

See [“How replication works”](#) on page 724.

Replicating data without a schedule

Replication normally occurs according to the schedule that you set up when you added a replication partner during installation. The site with the smaller ID number initiates the scheduled replication. You might want replication to occur immediately.

If you use the Microsoft SQL Server database with more than one server, you can only initiate replication from the first server at that site.

See [“Setting up sites and replication”](#) on page 718.

Replicating data without a schedule

- 1 In the console, click **Admin**, and then click **Servers**.
- 2 Under **Servers**, expand **Replication Partners** and select the partner whose database you want to replicate immediately.
- 3 Under **Tasks**, click **Replicate Now**.
- 4 Click **Yes**.
- 5 Click **OK**.

Replicating data on a schedule

Replication normally occurs according to the schedule that you set up when you added a replication partner during the initial installation. The site with the smaller ID number initiates the scheduled replication. When a replication partner has been established, you can change the replication schedule. When you change the schedule on a replication partner, the schedule on both sides is the same after the next replication.

The time that it takes to replicate depends on the size of the database as well as network connection between the sites. First, test a replication cycle to see how long it takes. You should schedule your replication based on that time period, and make sure that the time when the management servers duplicate data does not overlap.

After the initial, full database replication, subsequent replications are fairly small, if you only replicate policies, clients, and groups, and not logs.

See [“Setting up sites and replication”](#) on page 718.

Replicating data on a schedule

- 1 In the console, click **Admin**, and then click **Servers**.
- 2 Under **Servers**, click **Replication Partners**.
- 3 Under **Tasks**, click **Edit Replication Partner**.
- 4 In the **Edit Replication Partner** dialog box, specify the schedule for replication between the two partners by doing one of the following:
 - Check **Autoreplicate**.
It causes frequent and automatic replication to occur between two sites. This option is the default setting. Therefore you cannot set up a custom schedule for replication.

Note: The **Autoreplicate** option performs the replication process every two hours. Previous versions of the product automatically replicated every five minutes.

 - Uncheck **Autoreplicate**.
You can now set up a custom schedule for replication.
 - Select the hourly, daily, or weekly **Replication Frequency**.
 - Select the specific day during which you want replication to occur in the **Day of Week** list to set up a weekly schedule.
- 5 Click **OK**.

Specifying which data to replicate

You can choose to replicate or duplicate client packages, LiveUpdate content, and the logs between the local site and the remote site. The administrator at the remote site can then deploy the client package and LiveUpdate content.

If you decide to replicate client packages and LiveUpdate content, you may duplicate a large volume of data. The data in a client package might be as large as 5 GB. The 32-bit and 64-bit installation packages may require as much as 500 MB of disk space. If you plan to replicate logs, make sure that you have sufficient disk space for the additional logs on all the replication partner servers.

To specify which data to replicate

- 1 In the console, click **Admin**, and then click **Servers**.
- 2 Under **Servers**, click **Replication Partners**.
- 3 Expand **Replication Partners** and select the replication partner with which you want to replicate client packages.
- 4 Under **Tasks**, click **Edit Replication Partner Properties**.
- 5 In the **Replication Partner Properties** dialog box, click **Replicate client packages and LiveUpdate content between local site and partner site**.
- 6 Click **OK**.

See [“About client installation methods”](#) on page 115.

Deleting replication partners

The second management server that you replicate data with is classified as a remote site and called a replication partner. When you remove a management server at a remote site, you need to manually delete it from all sites. Uninstalling the software from one management server console does not make the icon disappear from the **Servers** pane on other consoles.

To delete a replication partner

- 1 In the console, click **Admin**.
- 2 Under **Tasks**, click **Servers**.
- 3 Expand **Remote Sites** and select the site that you plan to delete.
- 4 Under **Tasks**, click **Delete Remote Site**.
- 5 Click **Yes**.

See [“Re-adding a replication partner that you previously deleted”](#) on page 730.

See [“Setting up sites and replication”](#) on page 718.

Re-adding a replication partner that you previously deleted

You can add a replication partner that was previously deleted as a partner. For example, you must delete replication partners before you migrate or upgrade to the latest version of the management server. Later you can add that replication partner back to make the databases consistent. However, some changes may collide. If you add a deleted partner, the management server to which you want to connect must have previously been a partner in the same site farm.

To re-add a replication partner that you previously deleted

- 1 In the console, click **Admin**, and then click **Servers**.
- 2 Under **Servers**, select a site.
- 3 Under **Tasks**, click **Add Existing Replication Partner**.
- 4 In the **Specify Existing Replication Partner Wizard**, click **Next**.
- 5 In the **Remote Site Information** panel, type the IP address or host name and the port number of the management server that is the replication partner.
- 6 Type the administrator’s user name and password for the remote management server, and then click **Next**. You must use System administrator credentials.
- 7 In the **Schedule Replication** panel, specify the schedule for replication between the two partners by doing one of the following:
 - Check **Autoreplicate**.
It causes frequent and automatic replication to occur between two sites.
 - To set up a custom schedule for replication, check **Autoreplicate**, and specify the schedule.
- 8 Click **Next**.
- 9 In the **Replication of Log Files and Client Packages** panel, check or uncheck the options depending on whether or not you want to replicate logs.
- 10 In the **Add Replication Partner** dialog box, do one of the following:
 - If the database has been restored on the replication partner site, click **Yes**. You must restore the database on each replication partner site before you continue if you upgrade or restore a database.
 - Click **No** if the database has not been restored. Then restore the database and restart this procedure.

11 Click **Next**.

12 Click **Finish**.

The replication partner is added under **Replication Partners** on the **Admin** page.

See [“Turning off replication before an upgrade from Symantec Endpoint Protection 11.0”](#) on page 155.

See [“Turning on replication after an upgrade from Symantec Endpoint Protection 11.0”](#) on page 155.

See [“Deleting replication partners”](#) on page 729.

See [“Setting up sites and replication”](#) on page 718.

Preparing for disaster recovery

This chapter includes the following topics:

- [Preparing for disaster recovery](#)
- [Backing up the database and logs](#)
- [Backing up a server certificate](#)

Preparing for disaster recovery

In case of hardware failure or database corruption, you should back up the information that is collected after you install Symantec Endpoint Protection Manager. You then copy these files to another computer.

Table 37-1 High-level steps to prepare for disaster recovery

Step	Action	Description
Step 1	Back up the database	<p>Back up the database regularly, preferably weekly.</p> <p>By default, the database backup folder is saved to the following location:</p> <p><i>Symantec Endpoint Protection Manager installation folder\data\backup</i></p> <p>The backup file is called <i>date_timestamp.zip</i>.</p> <p>See “Backing up the database and logs” on page 733.</p>

Table 37-1 High-level steps to prepare for disaster recovery (*continued*)

Step	Action	Description
Step 2	Back up the disaster recovery file Update or back up the server certificate (optional)	<p>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:</p> <pre><i>Symantec Endpoint Protection Manager installation folder\Server Private Key Backup\recovery_timestamp.zip</i></pre> <p>Note: The recovery file only stores the default domain ID. If you have multiple domains, the recovery file does not store that information. If you need to perform disaster recovery, you must re-add the domains.</p> <p>See “Adding a domain” on page 311.</p> <p>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.</p> <p>See “Updating or restoring a server certificate” on page 690.</p> <p>See “Backing up a server certificate” on page 735.</p>
Step 3	Save the IP address and host name of the management server to a text file (optional)	<p>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.</p> <p>Add the IP address and host name to a text file, such as:</p> <pre><i>Backup.txt</i></pre>
Step 4	Copy the files you backed up in the previous steps to another computer	Copy the backed up files to a computer in a secure location.

See [“Performing disaster recovery”](#) on page 737.

See [“Backing up your license files”](#) on page 103.

See the knowledge base article [Best Practices for Disaster Recovery with the Symantec Endpoint Protection Manager](#).

See [“Exporting and importing server settings”](#) on page 695.

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: *Symantec Endpoint Protection Manager installation folder\data\backup*.

The backups are placed in a .zip file. By default, the backup database file is named *date_timestamp.zip*, the date on which the backup occurs.

Note: Avoid saving the backup file in the product installation directory. Otherwise, the backup file is removed when the product is uninstalled.

Log data is not backed up unless you configure Symantec Endpoint Protection Manager to back it up. If you do not back up the logs, then only your log configuration options are saved during a backup. You can use the backup to restore your database, but the logs in the database are empty of data when they are restored.

You can keep up to 10 versions of site backups. You should ensure that you have adequate disk space to keep all your data if you choose to keep multiple versions.

The database backup might take several minutes to complete. You can check the System log as well as the backup folder for the status during and after the backup.

You can back up the database immediately, or schedule the backup to occur automatically. You can back up an embedded database or a Microsoft SQL Server database that is configured as the Symantec Endpoint Protection Manager database.

See [“Scheduling automatic database backups”](#) on page 702.

See [“Preparing for disaster recovery”](#) on page 732.

To back up the database and logs

- 1 On the computer that runs Symantec Endpoint Protection Manager, on the **Start** menu, click **All Programs > Symantec Endpoint Protection Manager > Symantec Endpoint Protection Manager Tools > Database Back Up and Restore**.
- 2 In the **Database Back Up and Restore** dialog box, click **Back Up**.
- 3 In the **Back Up Database** dialog box, optionally check **Backup logs**, and then click **Yes**.
- 4 Click **OK**.
- 5 When the database backup completes, click **Exit**.
- 6 Copy the backup database file to another computer.

To back up the database and logs from within the console

- 1 In the console, click **Admin**, and then click **Servers**.
- 2 Under **Servers**, click the icon that represents the database.

- 3 Under **Tasks**, click **Back Up Database Now**.
- 4 In the **Back Up Database** dialog box, optionally check **Backup logs**, and then click **Yes**.
- 5 Click **OK**.
- 6 Click **Close**.

Backing up a server certificate

In case the computer on which the management server is installed gets corrupted, you should back up the private key and the certificate.

The JKS Keystore file is backed up during the initial installation. A file that is called `server_timestamp.xml` is also backed up. The JKS Keystore file includes the server's private and public key pair and the self-signed certificate.

To back up a server certificate

- 1 In the console, click **Admin**, and then click **Servers**.
 - 2 Under **Servers**, click the management server whose server certificate you want to back up.
 - 3 Under **Tasks**, click **Manage Server Certificate**, and then click **Next**.
 - 4 In the **Manage Server Certificate** panel, click **Back up the server certificate** and then click **Next**.
 - 5 In the **Back Up Server Certificate** panel, click **Browse** to specify a backup folder, and then click **Open**.
- Note that you back up the management server certificate into the same folder.
- 6 In the **Backup Server Certificate** panel, click **Next**.
 - 7 Click **Finish**.

See [“About server certificates”](#) on page 687.

Troubleshooting Symantec Endpoint Protection Manager

- [Chapter 38. Performing disaster recovery](#)
- [Chapter 39. Troubleshooting installation and communication problems](#)
- [Chapter 40. Troubleshooting reporting issues](#)
- [Chapter 41. Using Power Eraser to troubleshoot difficult and persistent threats](#)

Performing disaster recovery

This chapter includes the following topics:

- [Performing disaster recovery](#)
- [Reinstalling or reconfiguring Symantec Endpoint Protection Manager](#)
- [Generating a new server certificate](#)
- [Restoring the database](#)

Performing disaster recovery

[Table 38-1](#) lists the steps to recover your Symantec Endpoint Protection environment in the event of hardware failure or database corruption.

Note: This topic assumes that you have prepared for disaster recovery and have created backups and recovery files.

Table 38-1 Process for performing disaster recovery

Step	Action
Step 1	<p>Reinstall Symantec Endpoint Protection Manager using a disaster recovery file.</p> <p>By reinstalling the management server, you can recover the files that were saved after initial installation.</p> <p>See “Reinstalling or reconfiguring Symantec Endpoint Protection Manager” on page 738.</p> <p>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.</p> <p>See “Generating a new server certificate” on page 740.</p>
Step 2	<p>Restore the database.</p> <p>See “Restoring the database” on page 740.</p>

See [“Preparing for disaster recovery”](#) on page 732.

See the knowledge base article: [Disaster recovery best practices for Symantec Endpoint Protection 12.1](#).

Reinstalling or reconfiguring Symantec Endpoint Protection Manager

If you need to reinstall or reconfigure the management server, you can import all your settings by using a disaster recovery file. You can reinstall the software on the same computer, in the same installation directory.

You can also use this procedure to reconfigure the existing site, or to install an additional site for replication.

Symantec Endpoint Protection Manager creates a recovery file during installation. The recovery file is selected by default during the reinstallation process.

See [“Preparing for disaster recovery”](#) on page 732.

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 74.

- 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: *Symantec Endpoint Protection Manager installation folder\Server Private Key Backup*.

- 4 Follow the instructions in each panel. The default settings work for most cases. If the reinstalled server connects to an existing database, you change the database settings to those of the existing database.

You can also restore the database if necessary. However, if the Symantec Endpoint Protection Manager database resides on another computer or is otherwise not affected, you do not need to restore your database.

See [“Restoring the database”](#) on page 740.

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.

Generating a new server certificate

If you reinstall Symantec Endpoint Protection Manager on a different computer, you must generate a new server certificate.

If the original computer is corrupted or you upgrade the management server from a previous version, you must reinstall Symantec Endpoint Protection Manager on a different computer. To reinstall Symantec Endpoint Protection Manager on a different computer, you install the management server as if for the first time, rather than with the recovery file.

You reinstall the database settings on a different computer by using the database backup and restore utility. However, the server certificate that the new management server uses does not match the existing server certificate in the restored database. Because client-server communication uses the server certificate, you must generate a new server certificate.

See [“Reinstalling or reconfiguring Symantec Endpoint Protection Manager”](#) on page 738.

See [“Installing Symantec Endpoint Protection Manager”](#) on page 74.

To generate a new server certificate

- 1 In the console, click **Admin**, and then click **Servers**.
- 2 Under **Servers**, click the management server.
- 3 Under **Tasks**, click **Manage Server Certificate**, and then click **Next**.
- 4 In the **Manage Server Certificate** panel, click **Generate new server certificate** and then click **Next**.
- 5 Click **Yes**, and then click **Next**.

After you log on to Symantec Endpoint Protection Manager, you are asked to trust the new certificate.

See [“Logging on to the Symantec Endpoint Protection Manager console”](#) on page 78.

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 733.

You must restore the database using the same version of Symantec Endpoint Protection Manager that you used to back up the database. You can restore the database on the same computer on which it was installed originally or on a different computer.

The database restore might take several minutes to complete.

To restore the database

- 1 Stop the management server service.
See [“Stopping and starting the management server service”](#) on page 156.
- 2 On the **Start** menu, click **All Programs > Symantec Endpoint Protection Manager > Symantec Endpoint Protection Manager Tools > Database Back Up and Restore**.
- 3 In the **Database Back Up and Restore** dialog box, click **Restore**.
- 4 Click **Yes** to confirm the database restoration.
- 5 In the **Restore Site** dialog box, select the backup database file, and then click **OK**.
Locate the copy of the backup database file that you made when you backed up the database. By default, the backup database file is named *date_timestamp.zip*.
- 6 Click **OK**.
- 7 Click **Exit**.
- 8 Restart the management server service.

Troubleshooting installation and communication problems

This chapter includes the following topics:

- [Troubleshooting Symantec Endpoint Protection](#)
- [Troubleshooting computer issues with the Symantec Help support tool](#)
- [Identifying the point of failure of an installation](#)
- [Troubleshooting communication problems between the management server and the client](#)
- [Troubleshooting communication problems between the management server and the console or the database](#)
- [Client and server communication files](#)

Troubleshooting Symantec Endpoint Protection

[Table 39-1](#) displays the most common issues that you might encounter when you install and use Symantec Endpoint Protection.

Table 39-1 Common issues you can troubleshoot

Task	Description
Fixing installation problems	<p>You can download and run the Symantec Help (SymHelp) 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.</p> <p>See “Troubleshooting computer issues with the Symantec Help support tool” on page 744.</p> <p>See “Identifying the point of failure of an installation” on page 744.</p>
Handling virus outbreaks	<p>You can prevent threats from attacking computers on your network.</p> <p>See “Preventing and handling virus and spyware attacks on client computers” on page 399.</p> <p>See “Remediating risks on the computers in your network” on page 401.</p> <p>If a threat does attack a client computer, you can identify and respond to the threat. See the following knowledge base article:</p> <p>Best practices for troubleshooting viruses on a network.</p>
Troubleshooting content update problems	<p>If the latest virus definitions do not update correctly on Symantec Endpoint Protection Manager or the clients, see the following knowledge base article:</p> <p>Symantec Endpoint Protection: LiveUpdate Troubleshooting Flowchart.</p>
Fixing communication errors	<p>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.</p> <p>See “Troubleshooting communication problems between the management server and the client” on page 745.</p> <p>See “Troubleshooting communication problems between the management server and the console or the database” on page 754.</p>
Performing disaster recovery	<p>In case of database corruption or hardware failure, you can restore the latest snapshot of the database if you have a database backup file.</p> <p>See “Performing disaster recovery” on page 737.</p>
Reducing the space in the database	<p>You can make more space available on the database if the database size gets too large.</p> <p>See “Maintaining the database” on page 698.</p>
Troubleshooting reporting issues	<p>You can solve various report and log issues.</p> <p>See “Troubleshooting reporting issues” on page 758.</p>

Troubleshooting computer issues with the Symantec Help support tool

You can download a utility to diagnose common issues you encounter with installing and using Symantec Endpoint Protection Manager or the Symantec Endpoint Protection client.

The support tool helps you with the following issues:

- Lets you quickly and accurately identify known issues.
- When the tool recognizes an issue, the tool redirects you to the resources to resolve the issue yourself.
- When an issue is not resolved, the tool lets you easily submit data to Support for further diagnostics.

To troubleshoot computer issues with the Symantec Help support tool

- 1 Do one of the following tasks:
 - See the knowledge base article: [Symantec Help \(SymHelp\)](#)
 - In the console, click **Help > Download Support Tool**.
 - In the client, click **Help > Download Symantec Help 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 [“About client installation methods”](#) on page 115.

Troubleshooting communication problems between the management server and the client

If you have trouble with client and server communication, you should first check to make sure that there are no network problems. You should also check network connectivity before you call Symantec Technical Support.

You can test the communication between the client and the management server in several ways.

Table 39-2 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	<p>You can download and view the troubleshooting file on the client to verify the communication settings.</p> <p>See “How to determine whether the client computer is connected and protected” on page 169.</p> <p>See “Checking the connection to the management server on the client computer” on page 747.</p> <p>See “Investigating protection problems using the troubleshooting file on the client” on page 748.</p>

Table 39-2 Checking the connection between the management server and the client (*continued*)

What to check	Solution
<p>Test the connectivity between the client and the management server</p>	<p>You can perform several tasks to check the connectivity between the client and the management server.</p> <ul style="list-style-type: none"> ■ See “Enabling and viewing the Access log to check whether the client connects to the management server” on page 748. ■ Ping the management server from the client computer. See “Using the ping command to test the connectivity to the management server” on page 750. ■ 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 750.
<p>Check that the management server uses the correct server certificate</p>	<p>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.</p> <p>See “Updating or restoring a server certificate” on page 690.</p> <p>See “Best practices for updating server certificates and maintaining the client-server connection” on page 688.</p> <p>You can verify that the management server uses the wrong server certificate by checking the following items:</p> <ul style="list-style-type: none"> ■ The client does not display the green dot in the taskbar, which indicates that it does not communicate with the management server. See “How to determine whether the client is connected in the console” on page 167. ■ The client does not receive policy updates from the management server. ■ The management server shows that it does connect with the client. See “How to determine whether the client computer is connected and protected” on page 169.

Table 39-2 Checking the connection between the management server and the client (*continued*)

What to check	Solution
Check for any network problems	<p>You should verify that there are no network problems by checking the following items:</p> <ul style="list-style-type: none"> ■ 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	<p>You can use the debug log on the client to determine if the client has communication problems.</p> <p>See “Checking the debug log on the client computer” on page 751.</p> <p>See “Checking the inbox logs on the management server” on page 751.</p>
Recover lost client communication	<p>If the clients have lost the communication with a management server, you can use a tool to recover the communication file.</p> <p>See “Restoring client-server communication settings by using the SylinkDrop tool” on page 752.</p>

If Symantec Endpoint Protection Manager displays logging errors or HTTP error codes, see the following knowledge base article: [Symantec Endpoint Protection Manager Communication Troubleshooting](#).

Checking the connection to the management server on the client computer

If you have a managed client, you can check your connection to the management server. If you are not connected to the management server, you can request that your client connect.

See [“Troubleshooting communication problems between the management server and the client”](#) on page 745.

Checking the connection to the management server on the client computer

- 1 On the **Status** page, click **Help > Troubleshooting**.
- 2 In the **Troubleshooting** dialog box, click **Connection Status**.
- 3 In the **Connection Status** pane, you can see the last attempted connection and the last successful connection.
- 4 To reestablish a connection with the management server, click **Connect Now**.

Investigating protection problems using the troubleshooting file on the client

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

Symantec Technical Support might request that you email the `Troubleshooting.txt` file.

See [“Troubleshooting communication problems between the management server and the client”](#) on page 745.

To export the troubleshooting file from the client

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

You can save the file on the desktop or in a folder of your choice.

- 5 Using a text editor, open `Troubleshooting.txt` to examine the contents.

Enabling and viewing the Access log to check whether the client connects to the management server

You can view the Apache HTTP server Access log on the management server to check whether the client connects to the management server. If the client connects, the client's connection problem is probably not a network issue. Network issues include the firewall blocking access, or networks not connecting to each other.

You must first enable the Apache HTTP server Access log before you can view the log.

Note: Disable the log after you view it because the log uses unnecessary CPU resources and hard disk space.

See [“Troubleshooting communication problems between the management server and the client”](#) on page 745.

To enable the Apache HTTP server Access log

- 1 In a text editor, open the file *Symantec Endpoint Protection Manager installation folder\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 156.
 See [“Stopping and starting the Apache Web server”](#) on page 749.

To view the Apache HTTP server Access log

- 1 On the management server, open *Symantec Endpoint Protection Manager installation folder\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 748.

To stop the Apache Web server

- ◆ From a command prompt, type:

```
net stop semwebsrv
```

To start the Apache Web server

- ◆ From a command prompt, type:

```
net start semwebsrv
```

Using the ping command to test the connectivity to the management server

You can try to ping the management server from the client computer to test connectivity.

See [“Troubleshooting communication problems between the management server and the client”](#) on page 745.

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 [“How to determine whether the client computer is connected and protected”](#) on page 169.
- Checking the connection status on the Symantec Endpoint Protection client.
See [“Checking the connection to the management server on the client computer”](#) on page 747.

To use a browser to test the connectivity to Symantec Endpoint Protection Manager on the Symantec Endpoint Protection client

- 1 On the client computer, open a Web browser, such as Internet Explorer.
- 2 In the browser command line, type the following command:
http://management server address:8014/secars/secars.dll?hello,secars
 where *management server address* is the management server's DNS name, NetBIOS name, or IP address.
- 3 When the Web page appears, look for one of the following results:
 - If the word **OK** appears, the client computer connects to the management server. Check the client for a problem.
 - If the word **OK** does not appear, the client computer does not connect to the management server. Check the client's network connections and that network services are running on the client computer. Verify the DNS service for the client and check its routing path.
 See [“Troubleshooting communication problems between the management server and the client”](#) on page 745.

Checking the debug log on the client computer

You can check the debug log on the client. If the client has communication problems with the management server, status messages about the connection problem appear in the log.

See [“Troubleshooting communication problems between the management server and the client”](#) on page 745.

You can check the debug log by using the following methods:

- In the client, on the Help and Support menu, in the Troubleshooting dialog box, you can click **Edit Debug Log Settings** and type a name for the log. You can then click **View Log**.
- You can use the Windows registry to turn on debugging in the client. You can find the Windows registry key in the following location:
 HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\SMC\smc_debuglog_on

Checking the inbox logs on the management server

You can use a Windows registry key to generate logs about activity in the management server inbox. When you modify the Windows registry key, the

management server generates the logs (ersecreg.log and exsecars.log). You can view these logs to troubleshoot client and server communication.

See [“Troubleshooting communication problems between the management server and the client”](#) on page 745.

See [“Checking the debug log on the client computer”](#) on page 751.

To check the inbox logs on the management server

- 1 On the management server, under HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\SEPM, set the DebugLevel value to 3.

Typically, the inbox appears in the following location on the management server computer: *Symantec Endpoint Protection Manager installation folder\data\inbox\log*

- 2 Open the log with Notepad.

Restoring client-server communication settings by using the SylinkDrop tool

The Sylink.xml file includes communication settings between the client and a Symantec Endpoint Protection Manager server. If the clients have lost the communication with a management server, you must replace the old Sylink.xml file with a new Sylink.xml file. The SylinkDrop tool automatically replaces the Sylink.xml file on the client computer with a new Sylink.xml file.

Note: You can also replace the Sylink.xml file by redeploying a client installation package. Use this method for a large number of computers, for computers that you cannot physically access easily or computers that require administrative access.

See [“Restoring client-server communications with Communication Update Package Deployment”](#) on page 175.

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 134.

See [“Troubleshooting communication problems between the management server and the client”](#) on page 745.

Note: You must disable Tamper Protection to use the SylinkDrop.exe tool. You can also create a Tamper Protection exception for the SylinkDrop.exe tool.

See [“Changing Tamper Protection settings”](#) on page 494.

See [“Creating a Tamper Protection exception on Windows clients”](#) on page 509.

To recover 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 176.

- 2 Copy the communication file to the client computer.

You can either save the file to a network location, email it to the user on the client computer, or copy it to removable media.

- 3 Do one of the following tasks:

- On the installation file, locate `\Tools\SylinkDrop\SylinkDrop.exe`.
- On the computer that runs the management server, locate `drive:\Program Files (x86)\Symantec\Symantec Endpoint Protection\Version.Number\Bin\SylinkDrop.exe`

You can run the tool remotely or save it and then run it on the client computer. If you use the tool on the command line, read the SylinkDrop.txt file for a list of the tool's command parameters.

- 4 In the **Sylink Drop** dialog box, click **Browse**, and locate the .xml file you deployed in step 2 to the client computer.
- 5 Click **Update Sylink**.
- 6 When you see a confirmation dialog box, click **OK**.
- 7 In the **Sylink Drop** dialog box, click **Exit**.

Troubleshooting communication problems between the management server and the console or the database

If you have a connection problem with the console or the database, you may see one of the following symptoms:

- The management server service (semsrv) stops.
- The management server service does not stay in a started state.
- The Home, Monitors, and Reports pages display an HTTP error.
- The Home, Monitors, and Reports pages are blank.
- The Home, Monitors, and Reports pages display a continuously loading progress bar, without displaying any content.

All of these issues display a Java -1 error in the Windows Event log. To find the specific cause for the Java -1 error, look in the scm-server log. The scm-server log is typically located in the following location:

Symantec Endpoint Protection Manager installation
 folder\atomcat\logs\scm-server-0.log

Table 39-3 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 755.
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

Table 39-3 Checking the communication with the console or database
(continued)

What to check	Description
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 and System Requirements for all versions of Symantec Endpoint Protection and Symantec Network Access Control

Verifying the connection with the database

The management server and the database may not communicate properly. You should verify that the database runs and then test the connection between the server and the database.

If the management server runs the embedded Sybase database, perform the following steps:

- Verify that the Symantec Embedded Database service runs and that the dbdrv9.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 39-4 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 Threat Protection appears, and whether Windows services appear. When the client starts, it reads this file and returns to the same user interface state as before it was stopped.

Troubleshooting reporting issues

This chapter includes the following topics:

- [Troubleshooting reporting issues](#)
- [Changing timeout parameters for reviewing reports and logs](#)
- [Accessing reporting pages when the use of loopback addresses is disabled](#)

Troubleshooting reporting issues

You should be aware of the following information when you use reports:

- Timestamps, including client scan times, in reports and logs are given in the user's local time. The reporting database contains events in Greenwich Mean Time (GMT). When you create a report, the GMT values are converted to the local time of the computer on which you view the reports.
- If managed clients are in a different time zone from the management server, and you use the **Set specific dates** filter option, you may see unexpected results. The accuracy of the data and the time on both the client and the management server may be affected.
- If you change the time zone on the server, log off of the console and log on again to see accurate times in logs and reports.
- In some cases, the report data does not have a one-to-one correspondence with what appears in your security products. This lack of correspondence occurs because the reporting software aggregates security events.
- You can use SSL with the reporting functions for increased security. SSL provides confidentiality, the integrity of your data, and authentication between the client and the server.

See the knowledge base article: [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 759.
- If you get CGI or terminated process errors, you might want to change other timeout parameters.
For more information, see the following document in the knowledge base article: [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 762.

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 folder on the Symantec Endpoint Protection Manager server:

Drive: \Program Files\Symantec\Symantec Endpoint Protection Manager\Php\Include\Resources

On 64-bit operating systems, browse to the following folder:

Drive: \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** line and increase the value (in seconds). If the line does not exist, create it. For example, to increase the timeout period to 10 minutes, change the line to the following value:

`$CommandTimeout = 600;`

You must create the new line before the following characters: `?>`

- 4 Find the **\$ConnectionTimeout** line and increase the value (in seconds). If the line does not exist, create it. For example, to increase the timeout period to 10 minutes, change the line to the following value:

`$ConnectionTimeout = 600;`

- 5 Save and close the Reporter.php file.

Note: If you specify zero, or leave the fields blank, the default setting is used.

If you get CGI or terminated process errors, you might want to change the following parameters:

- `max_execution_time` parameter in the `Php.ini` file
- The Apache timeout parameters, `FcgidIOTimeout`, `FcgidBusyTimeout`, and `FcgidIdleTimeout`, in the `httpd.conf` file

To change the `max_execution_time` parameter in `Php.ini`

- 1 Browse to following folder on the Symantec Endpoint Protection Manager server:
Drive:\Program Files\Symantec\Symantec Endpoint Protection Manager\Php
On 64-bit operating systems, browse to the following folder:
Drive:\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 folder on the Symantec Endpoint Protection Manager server:
Drive:\Program Files\Symantec\Symantec Endpoint Protection Manager\apache\conf
On 64-bit operating systems, browse to the following folder:
Drive:\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 stand-alone Web browser”](#) on page 603.

To associate localhost with the IP address on computers running Windows

- 1 Change directory to the location of your hosts file.

By default, the hosts file is located in `%SystemRoot%\system32\drivers\etc`

- 2 Open the hosts file with an editor.
- 3 Add the following line to the hosts file:

```
xxx.xxx.xxx.xxx localhost #to log on to reporting functions
```

where you replace `xxx.xxx.xxx.xxx` with your computer's IP address. You can add any comment you want after the pound sign (#). For example, you can type the following line:

```
192.168.1.100 localhost # this entry is for my console computer
```

- 4 Save and close the file.

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](#)
- [Tasks to perform when you need to run Power Eraser from the Symantec Endpoint Protection Manager console](#)
- [Starting Power Eraser analysis from Symantec Endpoint Protection Manager](#)
- [Responding to Power Eraser detections](#)

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 SymHelp 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 SymHelp tool and run Power Eraser from the tool.

- If you use the SymHelp 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 SymHelp tool examines.

Note: Make sure that you do not run Power Eraser from the console and locally with the SymHelp 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 766.

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 480.
- 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 498.
- 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 miscellaneous settings for Virus and Spyware Protection on Windows computers”](#) on page 475.

- 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 129.

- 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 [“Enabling or disabling client submissions to Symantec Security Response”](#) on page 442.

- 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 [“Enabling or disabling client submissions to Symantec Security Response”](#) on page 442.

See [“Troubleshooting computer issues with the Symantec Help support tool”](#) on page 744.

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.

Tasks to perform when you need to run Power Eraser from the Symantec Endpoint Protection Manager console

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 763.

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 41-1 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	<p>To run Power Eraser on client computers, administrators must have the following command access rights:</p> <ul style="list-style-type: none"> ■ Start Power Eraser Analysis ■ Restart Client Computers (required to run Power Eraser with rootkit detection) <p>See “Adding an administrator account” on page 295.</p>
Set the log retention policy	<p>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.</p> <p>The log retention setting is part of the miscellaneous options in the Virus and Spyware Protection policy.</p> <p>See “Modifying miscellaneous settings for Virus and Spyware Protection on Windows computers” on page 475.</p>
Make sure that your clients have Internet connectivity	<p>Your client computers require Internet access so that Power Eraser can use Symantec Insight reputation data to make decisions about potential threats.</p> <p>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.</p>

Tasks to perform when you need to run Power Eraser from the Symantec Endpoint Protection Manager console

Table 41-1 Tasks to perform when you need to run Power Eraser from the Symantec Endpoint Protection Manager console (*continued*)

Task	Description
<p>Start a Power Eraser analysis on a client computer from Symantec Endpoint Protection Manager</p>	<p>Choose whether to run Power Eraser in regular mode or rootkit mode.</p> <p>You can issue the Power Eraser command from several places in Symantec Endpoint Protection Manager:</p> <ul style="list-style-type: none"> ■ Clients page ■ Computer Status log ■ Risk log <p>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 SymHelp 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.</p> <p>See “Starting Power Eraser analysis from Symantec Endpoint Protection Manager” on page 770.</p> <p>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.</p> <p>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.</p>
<p>Cancel a Power Eraser command or action on a client computer</p>	<p>To cancel the Power Eraser command, use the Command Status log.</p> <p>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.</p> <p>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.</p> <p>See “Running commands on client computers from the console” on page 261.</p>

Table 41-1 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	<p>You can view Power Eraser detections from the following logs in Symantec Endpoint Protection Manager:</p> <ul style="list-style-type: none"> ■ Scan log <p>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.</p> ■ Risk log <p>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.</p> ■ Computer Status log <p>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.</p> <p>A Power Eraser icon links to a report that shows any Power Eraser detections on the computer that require administrator action.</p> <p>These icons also appear in the Health Status column on the Clients page.</p> <p>See “Viewing logs” on page 613.</p>
Check for the notifications that recommend that you run Power Eraser on client computers	<p>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.</p> <p>See “Viewing and acknowledging notifications” on page 628.</p>
View Power Eraser detections on the Command Status page	<p>You can access reports about Power Eraser detections on the Command Status page.</p> <p>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.</p> <p>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.</p> <p>See “Running commands on client computers from the console” on page 261.</p>

Table 41-1 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	<p>You can access reports about Power Eraser detections from the Clients tab on the Clients page.</p> <p>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.</p> <p>A Power Eraser icon links to a report that shows any Power Eraser detections on the computer that require administrator action.</p> <p>The icons also appear in the Computer Status log.</p> <p>See “Viewing the protection status of clients and client computers” on page 253.</p>
Remediate or restore Power Eraser detections from the Scan log or Risk log in Symantec Endpoint Protection Manager	<p>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.</p> <p>You can also undo (restore) a Power Eraser detection that you remediated.</p> <p>See “Responding to Power Eraser detections” on page 772.</p>

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 763.

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 766.

See [“Responding to Power Eraser detections”](#) on page 772.

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 766.

See [“What you should know before you run Power Eraser from the Symantec Endpoint Protection Manager console”](#) on page 763.

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 41-2 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.

Client feature comparison tables

This appendix includes the following topics:

- [Client protection features based on platform](#)
- [Management features based on platform](#)
- [Virus and Spyware Protection policy settings based on platform](#)
- [Intrusion Prevention policy settings based on platform](#)
- [LiveUpdate policy settings based on platform](#)
- [Exceptions policy settings based on platform](#)

Client protection features based on platform

[Table A-1](#) lists which protection features are available on Windows clients, Mac clients, and Linux clients.

Table A-1 Client protection features based on platform

Client feature	Windows	Mac	Linux (12.1.5 and later)
Virus and Spyware Protection	Yes	Yes	Yes

Table A-1 Client protection features based on platform (*continued*)

Client feature	Windows	Mac	Linux (12.1.5 and later)
Network Threat Protection <ul style="list-style-type: none"> ■ Intrusion prevention ■ Firewall 	Yes	Yes (Intrusion prevention only; 12.1.4 and later) Note: Intrusion prevention for the Mac does not support custom signatures.	No
Proactive Threat Protection <ul style="list-style-type: none"> ■ Application and Device Control ■ SONAR and legacy TruScan 	Yes	No	No
Host Integrity	Yes	No	No
Other protections <ul style="list-style-type: none"> ■ System lockdown ■ Tamper Protection 	Yes	No	No

See [“About application and device control”](#) on page 523.

See [“How Host Integrity works”](#) on page 571.

See [“Configuring system lockdown”](#) on page 541.

See [“Management features based on platform”](#) on page 776.

See [“Virus and Spyware Protection policy settings based on platform”](#) on page 781.

See [“LiveUpdate policy settings based on platform”](#) on page 785.

See [“Exceptions policy settings based on platform”](#) on page 786.

See [“Intrusion Prevention policy settings based on platform”](#) on page 784.

Management features based on platform

[Table A-2](#) lists the management features that are available on Windows clients, Mac clients, and Linux clients.

Table A-2 Management features based on platform

Management feature	Windows	Mac	Linux (12.1.5 and later)
Deploy clients remotely from Symantec Endpoint Protection Manager <ul style="list-style-type: none"> ■ 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	<ul style="list-style-type: none"> ■ Scan ■ Update content ■ Update content and scan ■ Start Power Eraser analysis (12.1.5 and later) ■ Restart client computers ■ Enable Auto-Protect ■ Enable Network Threat Protection ■ Disable Network Threat Protection ■ Enable Download Insight ■ Disable Download Insight ■ Collect File Fingerprint List (12.1.6) ■ Delete from Quarantine* ■ Cancel all scans* 	<ul style="list-style-type: none"> ■ Scan ■ Update content ■ Update content and scan ■ Restart client computers (hard restart only) ■ Enable Auto-Protect ■ Enable Network Threat Protection (12.1.4 and later) ■ Disable Network Threat Protection (12.1.4 and later) 	<ul style="list-style-type: none"> ■ Scan ■ Update content ■ Update content and scan ■ Enable Auto-Protect
Allow Insight lookups for threat detection	Yes	No	No
Enable learned applications and Network Application Monitoring	Yes	No	No

Table A-2 Management features based on platform (*continued*)

Management feature	Windows	Mac	Linux (12.1.5 and later)
Create locations and set security policies that apply by location	Yes	Yes	No Note: You can view the client's location by the command line, but the client does not automatically switch locations based on specific criteria.
Set restart options for clients	Yes	No	No
Quick reports and Scheduled reports	<ul style="list-style-type: none"> ■ Audit ■ Application and Device Control ■ Compliance ■ Computer status ■ Network Threat Protection ■ Risk ■ Scan ■ System 	<ul style="list-style-type: none"> ■ Computer status ■ Network Threat Protection ■ Risk ■ Scan 	<ul style="list-style-type: none"> ■ Audit ■ Computer status ■ Risk ■ Scan ■ System
Set size and retention options for logs that are maintained on the client computers	<ul style="list-style-type: none"> ■ System ■ Security and risk ■ Security ■ Traffic ■ Packet ■ Control 	<ul style="list-style-type: none"> ■ System ■ Security and risk ■ Security 	<ul style="list-style-type: none"> ■ System ■ Security and risk
Password protecting the client	Yes	No	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-2 Management features based on platform (*continued*)

Management feature	Windows	Mac	Linux (12.1.5 and later)
Configure client submissions of anonymous security information to Symantec	Yes	12.1.4 and later Note: 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 anonymous 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	<ul style="list-style-type: none"> ■ Management server lists ■ Communication mode (push or pull) ■ Set heartbeat interval ■ Upload learned applications ■ Upload critical events immediately ■ Set download randomization ■ Set reconnection preferences 	<ul style="list-style-type: none"> ■ Management server lists ■ Communication mode (push or pull) ■ Set heartbeat interval ■ Set download randomization ■ Set reconnection preferences 	<ul style="list-style-type: none"> ■ Management server lists ■ Communication mode (push or pull) ■ Set heartbeat interval

Table A-2 Management features based on platform (*continued*)

Management feature	Windows	Mac	Linux (12.1.5 and later)
Configure clients to use private servers <ul style="list-style-type: none"> ■ Advanced Threat Protection 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	No	No
Automatically uninstall existing third-party security software	Yes	No	No

* You can only run these commands when viewing logs in Symantec Endpoint Protection Manager.

See [“About commands that you can run on client computers”](#) on page 258.

See [“Using Intelligent Updater files to update content on Windows computers”](#) on page 227.

See [“Tasks to perform when you need to run Power Eraser from the Symantec Endpoint Protection Manager console”](#) on page 766.

See [“Monitoring the applications and services that run on client computers”](#) on page 331.

See [“Managing the client-server connection”](#) on page 165.

See [“Restoring client-server communications with Communication Update Package Deployment”](#) on page 175.

See [“Client protection features based on platform”](#) on page 775.

See [“Virus and Spyware Protection policy settings based on platform”](#) on page 781.

See [“LiveUpdate policy settings based on platform”](#) on page 785.

See [“Exceptions policy settings based on platform”](#) on page 786.

See [“Intrusion Prevention policy settings based on platform”](#) on page 784.

See [“Upgrading Windows clients by using AutoUpgrade in Symantec Endpoint Protection”](#) on page 158.

Virus and Spyware Protection policy settings based on platform

Table A-3 lists the differences in the settings that are available for Windows clients, Mac clients, and Linux clients.

Table A-3 Virus and Spyware Protection policy settings based on platform

Policy setting	Windows	Mac	Linux (12.1.5 and later)
Administrator-defined scans	<ul style="list-style-type: none"> ■ Scheduled scans (Active, Full, Custom) ■ On-demand scans ■ Triggered scans ■ Startup scans 	<ul style="list-style-type: none"> ■ Scheduled scans (Custom) ■ On-demand scans 	<ul style="list-style-type: none"> ■ Scheduled scans (Custom) ■ On-demand scans
Email scans	<ul style="list-style-type: none"> ■ Internet email Auto-Protect ■ Microsoft Outlook Auto-Protect ■ Lotus Notes Auto-Protect 	No	No
Retry missed scheduled scans	Yes	No	Yes
Randomized scheduled scans	Yes	No	No
What to scan	<ul style="list-style-type: none"> ■ Scan additional locations ■ Scan memory ■ Scan selected folders ■ Scan selected extensions ■ Scan storage migration locations ■ Scan files inside compressed files ■ Scan for security risks 	<ul style="list-style-type: none"> ■ Scan all or selected folders ■ Scan hard drives and removable drives ■ Scan files inside compressed files 	<ul style="list-style-type: none"> ■ Scan all files ■ Scan all or selected folders ■ Scan selected extensions ■ Scan files inside compressed files ■ Scan for security risks
User-defined scans	<ul style="list-style-type: none"> ■ Active scan ■ Full scan ■ Custom scan of individual folders, files, and extensions 	<ul style="list-style-type: none"> ■ Full scan ■ Custom scan of individual folders and files 	<ul style="list-style-type: none"> ■ Full scan ■ Custom scan of individual folders and files

Virus and Spyware Protection policy settings based on platform

Table A-3 Virus and Spyware Protection policy settings based on platform
(continued)

Policy setting	Windows	Mac	Linux (12.1.5 and later)
Auto-Protect	<ul style="list-style-type: none"> ■ 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 ■ 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 	<ul style="list-style-type: none"> ■ 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 <p>Scan on mount, current clients:</p> <ul style="list-style-type: none"> ■ Data disks ■ All other disks and devices <p>Scan on mount, legacy clients (12.1.3 and earlier):</p> <ul style="list-style-type: none"> ■ Data disks ■ All other disks and devices ■ Music or video disks ■ iPod players ■ Show progress during scan 	<ul style="list-style-type: none"> ■ 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
Define remediation actions for detections	<ul style="list-style-type: none"> ■ Clean (only applies to malware) ■ Quarantine ■ Delete ■ Leave alone (log only) <p>The actions apply to categories of malware and security risks that Symantec periodically updates.</p>	<ul style="list-style-type: none"> ■ Repair infected files ■ Quarantine files that cannot be repaired 	<ul style="list-style-type: none"> ■ Clean (only applies to malware) ■ Quarantine ■ Delete ■ Leave alone (log only)

Table A-3 Virus and Spyware Protection policy settings based on platform
(continued)

Policy setting	Windows	Mac	Linux (12.1.5 and later)
Set actions to take while a scan is running	<ul style="list-style-type: none"> ■ Stop the scan ■ Pause a scan ■ Snooze a scan ■ Scan only when the computer is idle 	(12.1.4 and later) <ul style="list-style-type: none"> ■ Stop the scan ■ Pause a scan ■ Snooze a scan ■ Scan only when the computer is idle 	No
Tune scan performance for scan speed or application speed	Yes	No	No
Download Insight	Yes	No	No
Shared Insight Cache	Yes	No	No
Bloodhound	Yes	No	No
SONAR	Yes	No	No
TruScan legacy client settings (11.0)	Yes	No	No
Early Launch Anti-Malware Driver	Windows 8 and later, and Windows Server 2012 and later	No	No
Power Eraser (12.1.5 and later)	Yes	No	No
Advanced Threat Protection (12.1.6)	Yes	No	No
Virtual Image Exception	Yes	No	No

See [“Preventing and handling virus and spyware attacks on client computers”](#) on page 399.

See [“Using Symantec Endpoint Protection in virtual infrastructures”](#) on page 635.

See [“Client protection features based on platform”](#) on page 775.

See [“Management features based on platform”](#) on page 776.

See [“LiveUpdate policy settings based on platform”](#) on page 785.

See [“Exceptions policy settings based on platform”](#) on page 786.

Intrusion Prevention policy settings based on platform

[Table A-4](#) displays the differences in the settings that are available for Windows clients and Mac clients.

Note: The Linux client does not support intrusion prevention.

Table A-4 Intrusion Prevention policy settings based on platform

Policy setting	Windows	Mac (12.1.4 and later)
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 <ul style="list-style-type: none"> ■ 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 client computers”](#) on page 380.
- See [“Client protection features based on platform”](#) on page 775.
- See [“Management features based on platform”](#) on page 776.
- See [“Virus and Spyware Protection policy settings based on platform”](#) on page 781.
- See [“LiveUpdate policy settings based on platform”](#) on page 785.
- See [“Exceptions policy settings based on platform”](#) on page 786.

LiveUpdate policy settings based on platform

[Table A-5](#) displays the differences in the LiveUpdate settings that are available for Windows clients, Mac clients, and Linux clients.

Table A-5 LiveUpdate policy settings based on platform

Policy setting	Windows	Mac	Linux (12.1.5 and later)
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	<ul style="list-style-type: none"> ■ Virus and spyware definitions ■ SONAR(12.1.3 and later) ■ IPS definitions (12.1.3 and later) 	Virus and spyware definitions Only for legacy clients (12.1.3 and earlier)	Virus and spyware definitions

Table A-5 LiveUpdate policy settings based on platform (*continued*)

Policy setting	Windows	Mac	Linux (12.1.5 and later)
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	<ul style="list-style-type: none"> ■ Frequency ■ Retry window ■ Download randomization ■ Run when computer is idle ■ Options for skipping LiveUpdate 	<ul style="list-style-type: none"> ■ Frequency ■ Download randomization 	<ul style="list-style-type: none"> ■ Frequency ■ Retry window ■ Download randomization
Use standard HTTP headers	Yes	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 [“Managing content updates”](#) on page 181.

See [“Using Intelligent Updater files to update content on Windows computers”](#) on page 227.

See [“Client protection features based on platform”](#) on page 775.

See [“Management features based on platform”](#) on page 776.

See [“Virus and Spyware Protection policy settings based on platform”](#) on page 781.

See [“Exceptions policy settings based on platform”](#) on page 786.

Exceptions policy settings based on platform

[Table A-6](#) displays the Exceptions policy settings.

Table A-6 Exceptions policy settings based on platform

Policy setting	Windows	Mac	Linux (12.1.5 and later)
Server-based exceptions	<ul style="list-style-type: none"> ■ Applications ■ Applications to monitor ■ Extensions ■ Files ■ Folders ■ Known risks ■ Trusted web domains ■ Tamper Protection exceptions ■ DNS or Host file change exceptions 	<ul style="list-style-type: none"> ■ Security risk exceptions for files or folders 	<ul style="list-style-type: none"> ■ Folders ■ Extensions
Client restrictions	<p>Restricts users from adding any of the following exceptions:</p> <ul style="list-style-type: none"> ■ Applications ■ Extensions ■ Files ■ Folders ■ Known risks ■ Trusted web domains ■ DNS or Host file changes 	No	No

See [“Managing exceptions in Symantec Endpoint Protection”](#) on page 495.

See [“Client protection features based on platform”](#) on page 775.

See [“Management features based on platform”](#) on page 776.

See [“Virus and Spyware Protection policy settings based on platform”](#) on page 781.

See [“LiveUpdate policy settings based on platform”](#) on page 785.

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](#)
- [About client installation features and properties](#)
- [Symantec Endpoint Protection command-line client installation properties](#)
- [Symantec Endpoint Protection command-line client features](#)
- [Windows Installer parameters](#)
- [Windows Security Center properties](#)
- [Command-line examples for installing the Windows client](#)
- [Installing Windows clients with Microsoft SCCM/SMS](#)
- [Installing Windows clients with an Active Directory Group Policy Object \(GPO\)](#)
- [Uninstalling client software with an Active Directory Group Policy Object](#)

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.

[Table B-1](#) displays the third-party software and tools that you can use to install the client

Table B-1 Third-party tools to install the client

Tool	Description
Windows Installer command-line tools	<p>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.</p> <p>See “About client installation features and properties” on page 790.</p> <p>See “About configuring MSI command strings” on page 791.</p> <p>See “About configuring Setaid.ini” on page 791.</p> <p>See “Symantec Endpoint Protection command-line client features” on page 793.</p> <p>See “Symantec Endpoint Protection command-line client installation properties” on page 792.</p> <p>See “Windows Installer parameters” on page 794.</p> <p>See “Command-line examples for installing the Windows client” on page 798.</p> <p>See “Windows Security Center properties” on page 796.</p>

Table B-1 Third-party tools to install the client (*continued*)

Tool	Description
Microsoft SMS 2003	<p>You can install the client by using Microsoft Systems Management Server.</p> <p>See “Installing Windows clients with Microsoft SCCM/SMS” on page 798.</p>
Windows Active Directory	<p>You can use the Windows 2000/2003/2008 Active Directory Group Policy Object if the client computers and are members of a Windows 2000/2003/2008 Active Directory domain. The client computers must also use a supported Windows operating system.</p> <p>See “Installing Windows clients with an Active Directory Group Policy Object (GPO)” on page 799.</p> <p>See “Uninstalling client software with an Active Directory Group Policy Object” on page 804.</p>
Virtualization software	<p>You can install the client in virtual environments.</p> <p>See “Supported virtual installations and virtualization products” on page 62.</p>

See [“Exporting client installation packages”](#) on page 124.

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 Symantec Support knowledge base article, [MSI command line reference for Symantec Endpoint Protection](#).

Note: The Windows Installer advertise function is unsupported. Setaid.ini-specified features and properties take precedence over MSI-specified features and properties. Feature and property names in MSI commands are case-sensitive.

See [“About configuring Setaid.ini”](#) on page 791.

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
Pop3Smtplib=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 793.

See [“Symantec Endpoint Protection command-line client installation properties”](#) on page 792.

See [“Windows Installer parameters”](#) on page 794.

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= <i>val</i>	<p>Determines whether LiveUpdate is run as part of the installation, where <i>val</i> is one of the following values:</p> <ul style="list-style-type: none"> ■ 1: Runs LiveUpdate during installation (default). ■ 0: Does not run LiveUpdate during installation. <p>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.</p>

Table B-2 Symantec Endpoint Protection client installation properties
(continued)

Property	Description
ENABLEAUTOPROTECT= <i>val</i>	Determines whether File System Auto-Protect is enabled after the installation is complete, where <i>val</i> is one of the following values: <ul style="list-style-type: none"> ■ 1: Enables Auto-Protect after installation (default). ■ 0: Disables Auto-Protect after installation.
CACHE_INSTALLER= <i>val</i>	Determines whether the installation files cache on the client, where <i>val</i> is one of the following values: <ul style="list-style-type: none"> ■ 1: Caches the installation files (default). ■ 0: Does not cache the installation files.
MIGRATESETTINGS= <i>val</i>	Determines the status of preserved settings in an upgrade scenario, where <i>val</i> is one of the following values: <ul style="list-style-type: none"> ■ 0: Does not preserve the settings or logs. ■ 1: Preserves all settings and logs. ■ 2: Preserves Sylink.xml and logs only.
ADDSTARTMENUICON= <i>val</i>	Determines whether or not to add the program to the Start Menu folder, where <i>val</i> is one of the following values: <ul style="list-style-type: none"> ■ 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

[Table B-3](#) lists the Symantec Endpoint Protection features can be installed by specifying them in `Setaid.ini` files and in MSI commands. Most features have a parent-child relationship. If you want to install a child feature that has a parent feature, you must also install the parent feature.

For both `setaid.ini` and MSI, if you specify a child feature but do not specify its parent feature, the child feature is installed. However, the feature does not work because the parent feature is not installed. For example, if you specify to install the Firewall feature but do not specify to install NTPMain, the firewall is not installed.

Table B-3 Symantec Endpoint Protection client features

Feature	Description	Required parent features
Core	Installs the files that are used for communications between clients and Symantec Endpoint Protection Manager. This feature is required.	none
SAVMain	Installs the virus, spyware, and basic download protection. Subfeatures install additional protection.	Core
Download	Installs the complete protection for downloaded files. Includes fully functional reputation scanning by Download Insight.	SAVMain
NotesSnapin	Installs the Lotus Notes Auto-Protect email feature.	SAVMain
OutlookSnapin	Installs the Microsoft Exchange Auto-Protect email feature.	SAVMain
Pop3SmtP	Installs the protection for POP3 and SMTP mail. Available only on 32-bit systems.	SAVMain
PTPMain	Installs the Proactive Threat Protection components.	Core
TruScan	Installs the SONAR scanning feature.	PTPMain
DCMain	Installs the Application Control and Device Control feature.	PTPMain
NTPMain	Installs the Network Threat Protection components.	Core
ITPMain	Installs the Network and Intrusion Prevention and Browser Intrusion Prevention feature.	NTPMain
Firewall	Installs the firewall feature.	NTPMain
LANG1033	Installs English resources.	Core

Windows Installer parameters

Symantec Endpoint Protection client installation packages use the standard Windows Installer parameters, as well as a set of extensions for command-line installation and deployment.

See the Windows Installer documentation for further information about the usage of standard Windows Installer parameters. You can also execute msiexec.exe from a command line to see the complete list of parameters.

Table B-4 Windows Installer parameters

Parameter	Description
Sep.msi (32-bit) Sep64.msi (64-bit)	The 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, <code>msiexec.exe /I "C:\path to\Sep.msi"</code> Required
/qn	Install silently. Note: When a silent deployment is used, the applications that plug into Symantec Endpoint Protection, such as Microsoft Outlook and Lotus Notes, must be restarted after installation.
/x ".msi file name"	Uninstall the specified components. Optional
/qb	Install with a basic user interface that shows the installation progress. Optional
/!v <i>logfile</i>	Create a verbose log file, where <i>logfile</i> is the name of the log file you want to create. Optional
PRODUCTINSTALLDIR= <i>path</i>	Designate a custom path on the target computer where <i>path</i> is the specified target directory. If the path includes spaces, enclose the path in quotation marks. Note: The default directory is C:\Program Files\Symantec\Symantec Endpoint Protection Optional

Table B-4 Windows Installer parameters (*continued*)

Parameter	Description
SYMREBOOT= <i>value</i>	<p>Controls a computer restart after installation, where <i>value</i> is a valid argument.</p> <p>The valid arguments include the following:</p> <ul style="list-style-type: none"> ■ 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. <p>Optional</p> <p>Note: Use ReallySuppress to suppress a restart when you perform a silent uninstallation of Symantec Endpoint Protection client.</p>
ADDLOCAL= <i>feature</i>	<p>Select the custom features to be installed, where <i>feature</i> 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.</p> <p>To add all appropriate features for the client installations, use the ALL command as in ADDLOCAL=ALL.</p> <p>See “Symantec Endpoint Protection command-line client features” on page 793.</p> <p>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.</p> <p>Optional</p>
REMOVE= <i>feature</i>	<p>Uninstall the previously installed program or a specific feature from the installed program, where <i>feature</i> is one of the following:</p> <ul style="list-style-type: none"> ■ <i>Feature</i>: 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. <p>Optional</p>

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. They do not apply to clients that run Windows Vista, and do not apply to Windows Action Center in Windows 7, Windows 8, or later.

Table B-5 Windows Security Center properties

Property	Description
WSCCONTROL= <i>val</i>	<p>Controls WSC where <i>val</i> is one of the following values:</p> <ul style="list-style-type: none"> ■ 0: Do not control (default). ■ 1: Disable one time, the first time it is detected. ■ 2: Disable always. ■ 3: Restore if disabled.
WSCAVALERT= <i>val</i>	<p>Configures the antivirus alerts for WSC where <i>val</i> is one of the following values:</p> <ul style="list-style-type: none"> ■ 0: Enable. ■ 1: Disable (default). ■ 2: Do not control.
WSCFWALERT= <i>val</i>	<p>Configures the firewall alerts for WSC where <i>val</i> is one of the following values:</p> <ul style="list-style-type: none"> ■ 0: Enable. ■ 1: Disable (default). ■ 2: Do not control.
WSCAUPUPDATE= <i>val</i>	<p>Configures the WSC out-of-date time for antivirus definitions where <i>val</i> is one of the following values:</p> <p>1 - 90: Number of days (default is 30).</p>
DISABLEDEFENDER= <i>val</i>	<p>Determines whether to disable Windows Defender during installation, where <i>val</i> is one of the following values:</p> <ul style="list-style-type: none"> ■ 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
<p>Silently install all of the Symantec Endpoint Protection client components with default settings to the directory C:\SFN.</p> <p>Suppress a computer restart, and create a verbose log file.</p>	<pre>msiexec /I SEP.msi PRODUCTINSTALLDIR=C:\SFN SYMREBOOT=ReallySuppress /qn /l*v c:\temp\msi.log</pre>
<p>Silently install the Symantec Endpoint Protection client with Virus and Spyware Protection, and with Network Threat Protection.</p> <p>Force a computer restart, and create a verbose log file.</p>	<pre>msiexec /I SEP.msi ADDLOCAL=Core,SAVMain,OutlookSnapin, Pop3Smtpt,ITPMain,Firewall SYMREBOOT=Force /qn /l*v c:\temp\msi.log</pre>

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 clients with Save Package”](#) on page 122.

[Table B-7](#) lists the tasks to create and distribute Symantec client software with SCCM/SMS.

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 791.

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 clients with Save Package”](#) on page 122.

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 clients with Save Package” on page 122.
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 801.
Step 4	Add computers to the organizational unit. See “Adding computers to an organizational unit to install software” on page 803.

See [“Uninstalling client software with an Active Directory Group Policy Object”](#) on page 804.

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 799.

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 799.

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 one of the following commands, and then press **Enter**.
 - On the computers that run Windows XP and later, type **gpupdate**.
 - On the computers that run Windows 2000, type **secdit /refreshpolicy machine_policy**.

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 clients with Save Package”](#) on page 122.

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 239.

See [“Exporting the client-server communications file \(Sylink.xml\) manually”](#) on page 176.

- 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 137.

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.

Command-line options for the Windows client

This appendix includes the following topics:

- [Running the Windows client using the smc command-line interface](#)
- [smc command error codes](#)

Running the Windows client using the `smc` command-line interface

You can run the Windows client service using the `smc` 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.

Table C-1 `smc` parameters

Parameter	Description
<code>smc -start*</code>	Starts the client service. Returns 0, -1
<code>smc -stop*\$</code>	Stops the client service and unloads it from memory. Returns 0, -1

Table C-1 *smc* parameters (continued)

Parameter	Description
<code>smc -checkinstallation</code>	Checks whether the <code>smc</code> client service is installed. Returns 0, -3
<code>smc -checkrunning</code>	Checks whether the <code>smc</code> client service is running. Returns 0, -4
<code>smc -disable -ntp</code>	Disables the Symantec Endpoint Protection firewall and Intrusion Prevent System.
<code>smc -dismissgui</code>	Closes the client user interface. The client still runs and protects the client computer. Returns 0
<code>smc -enable -ntp</code>	Enables the Symantec Endpoint Protection firewall and Intrusion Prevention System.
<code>smc -exportconfig*§</code>	Exports the client's configuration file to an <code>.xml</code> 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: <code>smc -exportconfig C:\My Documents\MyCompanyprofile.xml</code> Returns 0, -1, -5, -6

Table C-1 smc parameters (continued)

Parameter	Description
<p>smc -exportlog</p>	<p>Exports the entire contents of a log to a .txt file.</p> <p>To export a log, you use the following syntax:</p> <pre>smc -exportlog log_type 0 -1 output_file</pre> <p>where:</p> <p><i>log_type</i> is:</p> <ul style="list-style-type: none"> ■ 0 = System Log ■ 1 = Security Log ■ 2 = Traffic Log ■ 3 = Packet Log ■ 4 = Control Log <p>For example, you might type the following syntax:</p> <pre>smc -exportlog 2 0 -1 c:\temp\TrafficLog</pre> <p>Where:</p> <p>0 is the beginning of the file -1 is the end of the file</p> <p>You can export only the Control log, Packet log, Security log, System log, and Traffic log.</p> <p><i>output_file</i> is the path name and file name that you assign to the exported file.</p> <p>Returns 0, -2, -5</p>
<p>smc -exportadvrule*§</p>	<p>Exports the client's firewall rules to a .sar file. The exported rules can only be imported into an unmanaged client or a managed client in client control mode or mixed mode. The managed client ignores these rules in server control mode.</p> <p>You must specify the path name and file name. For example, you can type the following command:</p> <pre>smc -exportadvrule C:\myrules.sar</pre> <p>Returns 0, -1, -5, -6</p> <p>When you import configuration files and firewall rules, note that the following rules apply:</p> <ul style="list-style-type: none"> ■ You cannot import configuration files or firewall rule files directly from a mapped network drive.

Table C-1 smc parameters (continued)

Parameter	Description
<code>smc -importadvrule*\$</code>	<p>Adds the imported firewall rules to the client's list of existing firewall rules. These rules do not overwrite the existing rules. The client lists both existing rules and imported rules, even if each rule has the same name and parameters.</p> <p>You can import only firewall rules into an unmanaged client or a managed client in client control mode or mixed mode. The managed client ignores these rules in server control mode.</p> <p>To import firewall rules, you import a .sar file. For example, you can type the following command:</p> <pre>smc -importadvrule C:\myrules.sar</pre> <p>An entry is added to the System log after you import the rules.</p> <p>Returns 0, -1, -5, -6</p>
<code>smc -importconfig*\$</code>	<p>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.</p> <p>You must specify the path name and file name. For example, you can type the following command:</p> <pre>smc -importconfig C:\My Documents\MyCompanyprofile.xml.</pre> <p>Returns 0, -1, -5, -6</p>
<code>smc -importsymlink\$</code>	<p>Imports the client communications file (symlink.exe).</p>
<code>smc -p [password]\$</code>	<p>Used in conjunction with a command that requires a password, where [password] is the required password. For example:</p> <pre>smc -p [password] -importconfig</pre>
<code>smc -runhi</code>	<p>Runs a Host Integrity check.</p> <p>Returns 0</p>
<code>smc -showgui</code>	<p>Displays the client user interface.</p> <p>Returns 0</p>
<code>smc -updateconfig</code>	<p>Initiates a client-server communication to ensure that the client's configuration file is up-to-date.</p> <p>If the client's configuration file is out-of-date, <code>updateconfig</code> downloads the most recent configuration file and replaces the existing configuration file, which is <code>serdef.dat</code>.</p> <p>Returns 0</p>

§ Parameters that need a password. You password-protect the client in Symantec Endpoint Protection Manager.

See “[Password-protecting the client](#)” on page 273.

* Parameters that only members of the Administrators group can use if the following conditions are met:

- The client runs Windows 2003/XP/Vista, or Windows Server 2008 and users are members of the Windows Administrators group.
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.
- The client runs Windows 2003/XP and users are members of the Power Users group.

To run the Windows client 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 -p
```

Where: *p* is a parameter
Type the installation path to the `smc` service before the command. For example, on a 64-bit Windows system, type:

```
C:\Program Files (x86)\Symantec\Symantec Endpoint Protection\smc.exe
```
 - If the parameter needs a password, type one of the following lines:
 - `smc -p password -parameter`
 - `smc -parameter -p password`For example: `smc -p password -exportconfig c:\profile.xml`

See “[smc command error codes](#)” on page 810.

smc command error codes

[Table C-2](#) displays the error codes that the `smc` command returns when the required parameters are invalid or missing.

Table C-2 `smc` 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.
-3	<code>smc</code> client service is not installed.
-4	<code>smc</code> client service is not running.
-5	Invalid input file. For example, the <code>importconfig</code> , <code>exportconfig</code> , <code>updateconfig</code> , <code>importadv</code> , <code>exportadvrule</code> , and <code>exportlog</code> parameters require the correct path name and file name.
-6	Input file does not exist. For example, the <code>importconfig</code> , <code>updateconfig</code> , and <code>importadvrule</code> parameters require the correct path name, configuration file name (.xml) or firewall rules file name (.sar).

See [“Running the Windows client using the `smc` command-line interface”](#) on page 806.

Command-line options for the Virtual Image Exception tool

This appendix includes the following topics:

- [vietool](#)

vietool

`vietool` – Runs the Virtual Image Exception tool

SYNOPSIS

```
vietool.exe volume: --generate|clear|verify|hash [options ...]
```

DESCRIPTION

The `vietool` command marks the base image files on the volume that you specify by adding an attribute.

OPTIONS

`--generate`

Runs the Virtual Image Exception tool on all files on the volume specified. You cannot use this option with `--clear`.

For example: `vietool c: --generate`

`--verify`

Verifies that the Virtual Image Exception is set on all files on the specified volume. You cannot use this option with `--clear`.

For example: `vietool c: --verify`

`--clear`

Removes the Virtual Image Exception on all files on the volume specified.

For example: `vietool.exe c: --clear`

To delete a specific file: `vietool.exe c:\Users\Administrator\target.file --clear`

You can use a fully qualified path in place of the volume identifier to clear the Virtual Image Exception on a single file or the contents of a folder. Only one file name, folder name, or volume identifier per command line is allowed. You cannot use this command with `--generate`, `--verify`, or `--hash`.

You must restart the client after you run the `--clear` command.

`--hash`

Generates the hash value on all files on the volume specified.

The 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.

Syntax for custom intrusion prevention signatures and application control rules

This appendix includes the following topics:

- [Regular expressions in Symantec Endpoint Protection Manager](#)
- [About signature syntax and conventions](#)
- [Protocol type arguments](#)
- [TCP protocol arguments](#)
- [UDP protocol arguments](#)
- [ICMP protocol arguments](#)
- [IP protocol arguments](#)
- [Msg arguments](#)
- [Content arguments](#)
- [Optional content arguments](#)
- [Case-sensitivity](#)
- [HTTP decoding](#)
- [Offset and depth](#)
- [Streamdepth arguments](#)
- [Supported operators](#)

- [Sample custom IPS signature syntax](#)

Regular expressions in Symantec Endpoint Protection Manager

You can use regular expressions in the IPS signature content and application control rules. By default, the regular expressions are case-sensitive.

For IPS, regular expressions use the following format:

```
regexcontent="string value" (offset , depth)opt
```

offset	Specifies the start of the bytes in the packet data, from which the IPS engine matches the signature pattern.
depth	Specifies the length of the packet data in which the IPS engine matches the signature pattern.
opt	Includes the C and the H options. <ul style="list-style-type: none"> ■ The C option makes the expression not case-sensitive. ■ The H option specifies HTTP decoding. ■ If there is no option, the entire data packet is matched.

For both IPS and application control, regular expressions support the following characteristics:

- Multiple regexcontent
- Case-sensitivity
- Binary format. The format is \x or \X with two Hex digits, like \xA9.

Table E-1 Syntax for regular expressions

Symbol	Description
Character	Matches itself, unless it is one of the following special characters (metacharacters): .\ [\] * + ^ \$
.	Matches any character and means one or more.

Table E-1 Syntax for regular expressions (*continued*)

Symbol	Description
\	<p>Matches the character following it, except when followed by:</p> <ul style="list-style-type: none"> ■ A left round bracket or a right round bracket. ■ A left angle bracket or right angle bracket. ■ A digit from 1 to 9. <p>The \ character is used as an escape character for all other metacharacters as well as itself. When it is used in a set ([4]), the \ character is treated as an ordinary character.</p>
[set] [^set]	<p>Matches one of the characters in the set.</p> <p>If the first character in the set is “^”, it matches a character NOT in the set, i.e., it complements the set. A shorthand S-E is used to specify a set of characters S up to E, inclusive. The special characters “]” and “-” have no special meaning if they appear as the first chars in the set.</p> <p>For example:</p> <ul style="list-style-type: none"> ■ [a-z]: Matches any alphabetic character ■ [^]: Matches any character except] and - ■ [^A-Z]: Matches any character except alpha character ■ [a-z A-Z]: Matches any alphabetic character. It is the same as [a-z] or [A-Z]
*	<p>Any regular expression from [1] to [4] followed by a closure character (*) that matches zero or more matches of that form.</p>
+	<p>Same as *, except that + matches one or more</p>
\(<i>form</i> \)	<p>A regular expression in supported syntax, enclosed as \(<i>form</i>\), matches whatever <i>form</i> matches. The enclosure tags the form to be used with \<<i>digit from 1 to 9</i>> for pattern substitution. The tagged forms are numbered in sequence starting at the beginning of the syntax.</p> <p>For example:</p> <ul style="list-style-type: none"> ■ \(\xxx\) [1-3] matches xxx1 or xxx2 or xxx3
\< <i>digit from 1 to 9</i> >	<p>Matches whatever a previously tagged regular expression \(<i>form</i>\) matched. The digit indicates which tagged form to match.</p> <p>In the first example here, \(\xxx\) is tagged as 1. In the second example, \(\yy\) is tagged as 1, \(\zz\) is tagged as 2.</p> <ul style="list-style-type: none"> ■ \(\xxx\) [1-3] 1 matches xxx1xxx or xxx2xxx or xxx3xxx ■ \(\yy\) X \(\zz\) [1-3] 2 1 matches yyXzz1zzyy or yyXzz2zzyy or yyXzz3zzyy

Table E-1 Syntax for regular expressions (*continued*)

Symbol	Description
\< \>	A regular expression that starts with \< and/or ends with \> restricts the pattern matching to the beginning of a word and/or the end of a word. A word is defined to be a character string that begins and/or ends with the characters A-Z a-z 0-9 and <code>_</code> . It must also be preceded or followed by any character outside those mentioned. For example, the syntax: <code>.*\<Symantec.\>.*</code> matches <code>...ABC Symantec 123....</code>
N/A	A composite regular expression <code>xy</code> where <code>x</code> and <code>y</code> are in the form <code>[1]</code> to <code>[10]</code> matches the longest match of <code>x</code> followed by a match for <code>y</code> .
N/A ^ \$	A regular expression that starts with a <code>^</code> character and/or ending with a <code>\$</code> character, restricts the pattern matching to the beginning of the line, or the end of line [anchors]. Elsewhere in the pattern, <code>^</code> and <code>\$</code> are treated as ordinary characters.

About signature syntax and conventions

When you write the content for each IPS signature, you must use the following syntax:

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

You must begin each signature with the keyword `rule`, followed by the protocol type argument, protocol options, IP protocol options, msg arguments, and content arguments. The optional arguments are enclosed in square brackets. Type only the information within the brackets; do not type the brackets. Arguments that are followed by an ellipsis may be repeated. You provide the information for the arguments, by using the supported operators and the regular expressions.

See [“Protocol type arguments”](#) on page 819.

See [“IP protocol arguments”](#) on page 823.

See [“Msg arguments”](#) on page 826.

See [“Content arguments”](#) on page 827.

See [“Supported operators”](#) on page 830.

See [“Regular expressions in Symantec Endpoint Protection Manager”](#) on page 816.

Protocol type arguments

This part of the signature defines the protocol type by using the following syntax:

```
protocol-type
```

where `protocol-type` is one of the following parameters:

- `tcp`
- `udp`
- `icmp`

The protocol type must immediately follow the word `rule`.

For example:

```
rule udp
```

Each `tcp`, `udp`, and `icmp` protocol type supports its own set of optional arguments.

See [“TCP protocol arguments”](#) on page 819.

See [“UDP protocol arguments”](#) on page 821.

See [“ICMP protocol arguments”](#) on page 822.

TCP protocol arguments

For additional details on the TCP protocol, refer to RFC 793.

Table E-2 TCP protocol arguments

Attribute	Description	Syntax
source	Source TCP port	<p>source operator (value)</p> <p>where value is an unsigned 16-bit number from 0 to 65535.</p> <p>Example:</p> <p>source=(180,2100)</p> <p>The value must be enclosed in parentheses. A value of 0 (zero) indicates all ports.</p> <p>You can specify a range of ports by using a dash between two port values (for example 3-5 is ports 3, 4, and 5). Multiple ports can be specified by separating them with commas.</p>
dest	Destination TCP port	<p>dest operator (value)</p> <p>where value is an unsigned 16-bit number from 0 to 65535.</p> <p>For example:</p> <p>dest=(120,125)</p> <p>value must be enclosed in parentheses. A value of 0 (zero) indicates all ports.</p> <p>A range of ports can be specified by using a dash between two port values (for example 3-5 is ports 3, 4, and 5). Multiple ports can be specified by separating them with commas.</p>

Table E-2 TCP protocol arguments (*continued*)

Attribute	Description	Syntax
tcp_flag	TCP flags present in the packet	<p>tcp_flag operator flag [flag]...</p> <p>where flag is one of the following parameters:</p> <ul style="list-style-type: none"> ■ fin: end of data ■ syn: synchronize sequence numbers ■ rst: reset connection ■ psh: push function ■ ack: acknowledgement field significant ■ urg: urgent pointer field significant ■ 0: match all flags <p>For example:</p> <p>tcp_flag&ack ps</p> <p>Most tcp_flag tests use the & (bitwise and) operator as a mask (meaning that a packet must have the specified flags set but can also have other flags set).</p> <p>You can specify multiple flags in a test by placing a pipe character between the flags.</p>
window	TCP window size	<p>window operator size</p> <p>where operator size is an unsigned 16-bit number from 0 to 65535.</p> <p>For example:</p> <p>window=16384</p>

UDP protocol arguments

For additional details on UDP protocol, refer to RFC 768.

Table E-3 UDP protocol arguments

Attribute	Description	Syntax
source	Source UDP port	<p>source operator (value)</p> <p>where <i>value</i> is an unsigned 16-bit number from 0 to 65535.</p> <p>For example:</p> <p>source=(180,2100)</p> <p>The value must be enclosed in parentheses. A value of 0 (zero) indicates all ports.</p> <p>A range of ports can be specified by using a dash between two port values (for example 3-5 is ports 3, 4, and 5). Multiple ports can be specified by separating them with commas.</p>
dest	Destination UDP port	<p>dest operator (value)</p> <p>where <i>value</i> is an unsigned 16-bit number from 0 to 65535.</p> <p>For example:</p> <p>dest=(120)</p> <p>The value must be enclosed in parentheses. A value of 0 (zero) indicates all ports.</p> <p>A range of ports can be specified using a dash between two port values (for example 3-5 is ports 3, 4, and 5). Multiple ports can be specified by separating them with commas.</p>

ICMP protocol arguments

Refer to RFCs 792 and 1256 for detailed descriptions of valid ICMP protocol type and code combinations.

Table E-4 ICMP protocol arguments

Attribute	Description	Syntax
type	ICMP protocol type	<code>type operator value</code> where <code>value</code> is an unsigned 8-bit number from 0 to 255. For example: <code>type=0</code>
code	ICMP protocol type	<code>code operator value</code> where <code>value</code> is an unsigned 8-bit number from 0 to 255. For example: <code>code<=10</code>

IP protocol arguments

The IP protocol arguments are independent of the protocol type arguments and are valid for the TCP, UDP, and ICMP protocol types.

For additional details on IP protocol, refer to RFC 791.

Table E-5 IP protocol arguments

Attribute	Description	Syntax
saddr	Source IP address	<p>saddr=(value/CIDR)</p> <p>where:</p> <ul style="list-style-type: none"> ■ value is a standard 32-bit IP address or the variable \$LOCALHOST, which specifies the IP address of the client computer. ■ CIDR is a classless inter-domain routing notation that indicates how many bits are used for the network prefix. <p>For example:</p> <p>saddr=(127.0.0.0/25)</p> <p>Here, 25 bits are used to identify the unique network and the remaining bits that identify the host.</p>
daddr	Destination IP address	<p>daddr=(value/CIDR)</p> <p>where:</p> <ul style="list-style-type: none"> ■ value is an IP address or the variable \$LOCALHOST, which specifies the IP address of the computer that runs the client. ■ CIDR is a classless inter-domain routing notation that indicates how many bits are used for the network prefix. <p>For example:</p> <p>daddr=(128.0.0.0/4)</p> <p>Here, four bits are used to identify the unique network and the remaining bits that identify the host.</p>

Table E-5 IP protocol arguments (*continued*)

Attribute	Description	Syntax
tos	Type of service flag present in the packet	<p>tos operator value</p> <p>where <i>value</i> is a numeric constant in a decimal, hexadecimal, or octal format.</p> <p>For example:</p> <pre>tos=0x4</pre> <p>To view valid IP tos values, see Table E-6.</p> <p>To test for multiple IP tos values in a packet, the tos argument should be the sum of the values that are to be tested. Typically, the operator is either = or &. These flags cannot be combined by using the pipe character () as in tcp_flags.</p>
tot_len	Total length of the packet	<p>tot_len operator value</p> <p>where <i>value</i> is a 16-bit number from 0 to 65535 that specifies the total length of packet.</p> <p>For example:</p> <pre>tot_len>1445</pre> <p>When you specify the value, the rule protocol-type must be considered to properly calculate the length to be tested. To aid in calculating the tot_len for each of the supported protocol types, their header lengths are as follows:</p> <p>TCP: 20-60 bytes</p> <p>UDP: 8 bytes</p> <p>ICMP: 8-20 bytes</p>

Table E-5 IP protocol arguments (*continued*)

Attribute	Description	Syntax
ttl	Time-to-live (TTL) of the packet	ttl operator value where <i>value</i> is an 8-bit value from 0 to 255 that specifies the time-to-live characteristic of the packet.
ip_flag	Fragmentation offset value of the packet	ip_flag operator value where <i>value</i> is a 13-bit value that specifies the fragmented offset value in the packet. IP fragmentation offsets occur on 8-byte boundaries; therefore, each bit value in the fragmentation offset represents three bits.

Table E-6 Valid IP tos values

Dec	Hex	Option
2	0x2	Minimize monetary cost
4	0x4	Maximize reliability
8	0x8	Maximize throughput
24	0x18	Minimize delay

Msg arguments

When an IPS signature successfully matches packet content with the rule's test conditions, the message is specified in the msg argument. The msg argument appears in the Security Log on both the client and the server. Only one msg argument can be included in each IPS signature.

Syntax:

```
msg="alert message"
```

The alert message must be enclosed in double quotation marks and cannot contain punctuation. Single quotation marks are not allowed. The purpose of the alert message is to let you easily identify an event in your network by reviewing the

Security Log. Therefore, all IPS signatures must contain concise yet descriptive alert messages within the msg argument.

Example:

```
msg="IIS Unicode Transversal Vulnerability"
```

Content arguments

The content argument specifies a pattern to look for within a packet. The content argument can appear multiple times in an IPS signature. The content value must be enclosed in double quotation marks (" "). Single quotation marks (' ') are not allowed.

Syntax:

```
content="value"
```

where `value` is a pattern that is specified as a string literal or a binary literal that must be enclosed in quotation marks.

A string literal is a group of consecutive characters, including spaces. A string can contain any characters except a quotation mark ("), backslash (\), or newline character escape sequence (\n). Example:

```
content="system32"
```

A binary literal is a group of consecutive bytes expressed in hexadecimal format, where the escape sequence \x precedes each byte. Example:

```
content="\x04\x20\x20\x20\xBF"
```

The following example specifies the content as the binary literal "\x04\x20\x20\x20\xBF".

String literals can be combined with binary literals to create complex patterns.

Example:

```
content="\x0DLocation\x3A"
```

Optional content arguments

You can use additional optional content arguments to further qualify the content in the following ways:

- Case-sensitivity
- HTTP decoding
- Depth and offset

Case-sensitivity

You can specify an optional C case-sensitivity flag on each content argument. When the flag follows a content argument, the pattern that is contained in the content argument matches only if the case of the characters in the string matches the case of the data in the packet.

For example, you can use the following syntax:

```
content="value"C  
content="\x0DLocation\x3A"C
```

HTTP decoding

You can use the optional HTTP H decoding flag in each content argument. If you use the H HTTP decoding flag, encoded characters are converted into a binary literal before they try a pattern match. You can also use the HTTP H after a C case-sensitivity flag. HTTP URIs use encoded characters. When the pattern match is attempted and normalized, the normalized data is compared to the binary or the string literal in the content argument. Under most circumstances, the H flag is used only for the TCP rules that relate to an application that uses the HTTP protocol.

For example, you can use the following syntax:

```
content="value"H  
content="\x6f\x6e\x4c\x6f\x61\x64\x3d\x22\x61\x6c\x65\x72\x74\x28"H
```

Offset and depth

You can use the offset value and a depth value as optional arguments in the content. The offset value is specified first, followed by the depth value.

For example, you can use the following syntax:

```
content="value" (offset, depth)
```

Syntax	Description
value	A pattern that is specified as a string literal or a binary literal that must be enclosed in quotation marks.

Syntax	Description
<code>offset</code>	<p>A positive integer in decimal notation.</p> <p>The offset specifies an alternative location to begin a pattern match. The offset also specifies how many bytes to skip before the signature tries to pattern match.</p> <p>When an offset argument is not present or has a value of 0, the content argument pattern tries to find a match. The pattern tries to match the content at the beginning of the packet payload or the portion of the packet following the protocol header for the first content argument. Each successive content argument automatically begins to test for pattern matches that follow the end of the previous successful pattern match.</p>
<code>depth</code>	<p>A positive integer in decimal notation. The depth specifies the maximum number of bytes to search when trying to match a pattern in a content argument.</p> <p>When a depth argument has a value of 0, the pattern that is contained in the content argument tries to find a match from the offset to the end of the packet. The depth argument value cannot be smaller than the number of bytes that are specified as the pattern to match within the argument of the content argument.</p>

```
content="\x04\x20\x20\x20\xBF" (4, 5)
```

This example skips four bytes forward from the previous pattern match or from the beginning of the packet payload and compares the next five bytes with the binary literal that is contained in the content argument.

Streamdepth arguments

You can use the streamdepth argument to limit the length of the stream in which the intrusion prevention rule checks for a signature. You might want to use streamdepth to improve the performance of your custom intrusion prevention rules. The streamdepth argument is optional.

Syntax:

```
streamdepth=value
```

For example, you might suspect that a signature exists in the first 10KB of a 1MB stream. You can use the following syntax:

```
streamdepth=10240
```

On the file download, the intrusion prevention rule with this streamdepth value stops checking for the signature after 10KB. Since you limit the checking, the download performance is improved.

If you set streamdepth to 0, intrusion prevention applies the rule to the entire stream.

Supported operators

Many arguments in the signature syntax require an operator that indicates the type of test that is to be performed to check for this type of attempt.

[Table E-7](#) describes the supported operators.

Table E-7 Supported operators used in IPS signatures

Operator	Description
<	less than
>	greater than
=	equal to
&	bitwise and In the signature library, the ampersand character & is sometimes represented using its HTML equivalent &
<=	less than or equal to
>=	greater than or equal to

Sample custom IPS signature syntax

You can create sample custom IPS signatures to detect an attempt to access and download MP3 files through a Web browser or FTP.

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

To detect an MP3 file and then block access to it, you write two signatures. One signature detects an MP3 file through the HTTP service. The second signature detects an MP3 files through the FTP service.

When you create a custom IPS signature, you must type the content of the signature by using the following format:

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

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

Web browsers use the HTTP GET command to download MP3 files. The FTP client uses the FTP RETR command to download files. The FTP command is also used when multiple files are retrieved by using the MGET command. The file name and respective mp3 extension is present in both requests. Both protocols insert [CR][LF] characters to mark the end of the request

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

See [“Regular expressions in Symantec Endpoint Protection Manager”](#) on page 816.

The content of the HTTP signature contains the following syntax:

```
rule tcp, dest=(80,443), saddr=$LOCALHOST,  
msg="MP3 GET in HTTP detected",  
regexpcntent="[Gg][Ee][Tt] .*[Mm][Pp]3 ."
```

The content of the FTP signature contains the following syntax:

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

[Table E-8](#) explains the syntax for the HTTP signature and the FTP signature.

Table E-8 HTTP signature and FTP signature syntax

Use the following syntax	To perform the following task
<p>For the HTTP signature:</p> <pre>rule tcp dest=(80,443)</pre> <p>For the FTP signature:</p> <pre>rule tcp dest=(21)</pre>	<p>Tells the packet-based engine what traffic to search. This way, the engine does not search unnecessary traffic and does not use up system resources. The more detailed information you provide, the better the packet-based engine performs.</p> <p>This argument limits the destination ports to 80 and 443 for the HTTP service and to 21 for the FTP service.</p>
<p>For the FTP signature:</p> <pre>tcp_flag&ack</pre>	<p>Reduces the false positives.</p>
<pre>saddr=\$LOCALHOST</pre>	<p>Makes sure that the request originates on the host.</p>
<p>For the HTTP signature:</p> <pre>msg="MP3 GET in HTTP"</pre> <p>For the FTP signature:</p> <pre>msg="MP3 GET in FTP"</pre>	<p>Displays the name for the signature when the signature is triggered. The name appears in the Security Log. Use a descriptive string so that you can identify the triggered signature in the log.</p>
<p>For the HTTP signature:</p> <pre>regexcontent="[Gg][Ee][Tt].*[Mm][Pp]3.*"</pre> <p>For the FTP signature:</p> <pre>regexcontent="[Rr][Ee][Tt][Rr].*[Mm][Pp]3\x0d\x0a"</pre>	<p>Matches this string in the HTTP traffic or the FTP traffic with the payload in the TCP packets. To reduce false positives, use this argument carefully.</p> <p>The string matches the ASCII text of the TCP packet, which is "GET [.*].mp3[CR][LF]" for the HTTP signature and "RETR [.*].mp3[CR][LF]" for the FTP signature.</p> <p>The string is written so that the text can be case-insensitive.</p>

Index

A

- actions
 - scan detections 478
- Active Directory servers
 - connecting to 242
 - importing organizational units 244
 - importing user information from 240–241
- active response 345
- active scans
 - when to run 408
- adapters. *See* network adapters
- adding
 - groups 239
- administrator accounts
 - locking or unlocking 84
 - managing 291
- administrator-defined scan
 - customizing 469
- administrator-defined scans 461–463
 - See also* on-demand scans
 - See also* scheduled scans
 - on Linux computers 463
 - on Mac computers 462
 - on Windows computers 461
- administrators
 - access rights 293
 - add account 295
 - change password 305
 - rename 295
 - setting up authentication 297
 - testing account authentication 300
 - types of 293
- Advanced Threat Protection 457
- adware 413
- Apache
 - log 748
 - stopping and starting 749
- application
 - monitoring 507
 - using an except to allow or block 507
 - using an exception to detect 507
 - application and device control log 615
- Application and Device Control Policies
 - structure 525
- application control
 - about 523
 - adding rules 535
 - best practices 531
 - creating a custom rule set 535
 - creating custom rules 529
 - custom rules 539
 - default rule sets 528
 - rules for specific applications 537
 - setting up 526
 - testing 540
 - typical rules 533
- application control rules
 - copying between policies 536
 - regular expressions 816
- application name list 553
- application triggers
 - firewall rules 356
- applications 356
 - See also* learned applications
 - searching for 333
- assistive technology
 - creating exceptions for 502
- attacks
 - blocking 345
- audit log 615
- audit signatures 380
- authentication
 - peer-to-peer 582
 - setting up for administrators 297–298
 - testing administrator accounts 300
- Auto-Protect
 - customizing for email scans 468
 - customizing for Linux computers 466
 - customizing for Mac computers 465
 - customizing for Windows clients 464
 - Download Insight 257
 - enabling or disabling 257

- Auto-Protect (*continued*)
 - for file system
 - enabling 260
 - automatic exclusions
 - about 414
 - for Microsoft Exchange server 415
 - for Symantec products 416
 - AutoUpgrade
 - client 158
 - availability
 - for databases and management servers 713
 - avoiding a restart 263
- B**
- blacklist
 - updating automatically 554, 558
 - updating for system lockdown 557
 - blacklist mode
 - enabling for system lockdown 562
 - blended threats 413
 - blocking
 - attacking computers 345
 - clients from groups 248
 - Bloodhound
 - modifying settings 474
 - bots 413
 - browser intrusion prevention
 - about 383
 - feature dependencies 437
- C**
- certificate
 - generating new 740
 - JKS keystore file 687
 - keystore file 688
 - update 690
 - CGI errors
 - database 760
 - client
 - Client Deployment Wizard 115
 - commands 806, 810
 - deployment 115, 118, 120, 122
 - install features 117
 - installation 115, 118, 120, 122
 - installing on Linux 132
 - installing on Mac 130
 - managed and unmanaged 134
 - package replication 729
 - client (*continued*)
 - password protection 273
 - remote deployment 111
 - uninstalling on Linux 139
 - uninstalling on Mac 138
 - uninstalling on Windows 137
 - updates
 - Intelligent Updater 227
 - third-party distribution tools 228
 - user interface
 - access to 266
 - configuring 270
 - client computer
 - disabled 597
 - group assignment 248
 - installation settings 126
 - moving to group 248
 - offline 597–598
 - online 597
 - policy updates 169
 - preparing for installation 108
 - status 597
 - system protection 597
 - troubleshooting 748
 - unmanaged on Windows 136
 - unscanned 598
 - upgrading to a new release 145
 - client connection. *See* health state
 - status icon 167
 - client control 268
 - client features
 - comparison 775
 - client installation packages
 - about 140
 - adding updates 142
 - collecting user information 272
 - configuring 127
 - exporting 124
 - client software installed
 - displaying 254
 - client status
 - viewing 253
 - client user interface
 - configuring 267
 - client-server communication settings
 - exporting 176
 - importing 178
 - client-server communications
 - fixing 174

- clients
 - deployment status 254
 - disabling protection on 256
 - purging in non-persistent virtual desktop infrastructures 678
- collect user information 272
- command line 813
- commands 813
 - client 806, 810
 - running from logs 261
 - running on clients from the console 261
- communication
 - problems between the client and the server 745
 - problems with the server and the console or the database 754
- communication and required ports 113
- communication settings
 - client and server 757
- communications file
 - replacing 174
- components
 - product 50
- computer status
 - logs 616
 - viewing 253
- computers
 - search for 255
 - updating protection on 181
- connectivity
 - communication between the client and the server 745
 - using a browser to test 750
 - using ping to test 750
 - verifying communication with the database 755
- console
 - about 86
 - timeout 85
- content
 - about storing revisions 190
 - how clients receive updates 182
 - managing updates 181
 - randomizing 206
 - replication 729
 - revisions that are not the latest version 205
- control levels 267
- converting an unmanaged client to a managed client 173
- custom IPS signatures
 - managing 391

- custom IPS signatures *(continued)*
 - testing 397

D

- database
 - backing up 702, 733
 - CGI errors 760
 - changing timeout parameters 759
 - errors 759
 - maintaining 698
 - restoring 740
 - terminated process errors 760
- databases
 - availability 713
- dba password
 - change 305
- debug logs. *See* logs
- Default Group 236
- definitions
 - updating 181
- definitions files
 - configuring actions for new definitions 449
- deploying
 - clients 118, 120, 122
- deployment status 254, 600
- device control
 - about 523
 - configuring 569
 - hardware devices list 566
 - setting up 526
- device ID
 - obtaining 567
- DHCP traffic 343
- dialers 413
- disable
 - Auto-Protect 257
 - Network Threat Protection 258
 - Proactive Threat Protection 257
- disaster recovery
 - about the process 737
 - preparing for 732
 - reinstalling server 738
- DNS queries
 - based on location 363
- DNS traffic 343
- domain
 - log on banner 82
- domain administrator 293

- domains
 - about 309
 - adding 311
 - copying clients and policies 310
 - disabling 310
 - managing 291
- Download Insight
 - actions 477
 - customizing settings 477
 - feature dependencies 437
 - interaction with Auto-Protect 257
 - managing detections 432
 - notifications 477
 - reputation data 436
- Download Protection
 - feature dependencies 437
- E**
- early launch anti-malware
 - adjusting options 455
 - detections 454
- ELAM. *See* early launch anti-malware
 - disable to improve computer performance 427
- email application inbox
 - exclusion for 417
- email messages
 - for firewall rules 377
- email server
 - link to management server 628
- Embedded client
 - client installation package 114
- embedded database
 - installation settings 65
- endpoint protection
 - monitoring 597, 599
 - status 597–598
- event logs 613
 - past 24-hours filter 617
- exceptions 497
 - client restrictions 511
 - creating 498
 - DNS or host file change 510
 - excluding a file or folder 503
 - file extensions 506
 - from log events 512
 - known risks 505
 - managing 495
 - platform comparison 786
 - Tamper Protection 509
- excluded hosts 389
- exclusions
 - created automatically 414
- expiring passwords
 - enabling 308
- exporting
 - client installation packages 124
 - firewall rules 369
 - policies 326
- external logging 706
- F**
- failover
 - defined 713
- failover and load balancing
 - configuring 715
- feature dependencies 437
- file fingerprint list
 - importing or merging 550
 - updating manually 551
- file sharing 375
- File System Auto-Protect. *See* Auto-Protect
- filters
 - saving in logs 617
- firewall 336–338
 - disabling Windows firewall 347
 - enabling and disabling 342
 - notifications 360
 - policies 339
 - stateful inspection 355
 - traffic settings 346–347
- firewall rules 370
 - about 348, 350
 - adding 368
 - allowing traffic to local subnet 374
 - applications 356
 - adding 356
 - block by IP address
 - adding 373
 - email messages 377
 - host groups
 - creating 362
 - hosts 360
 - importing and exporting 369
 - inheriting 352, 354
 - network adapter triggers 365
 - network adapters
 - adding 366, 378
 - network service triggers 364

- firewall rules (*continued*)
 - network services 364
 - adding 375
 - processing order
 - about 351
 - changing 354
 - scheduling 379
 - setting up 367
- forgotten password
 - reset 307
- full scans
 - when to run 408

G

- global scan settings 474
- group
 - computer assignment 248
- Group Update Provider
 - controlling content downloads 223
 - explicit list 216, 223
 - legacy clients 216
 - managing 215
 - multiple 216, 222–223
 - searching for 226
 - single 216, 223
 - types 216
- groups
 - adding 239
 - assigning management server list 716
 - blocking 248
 - importing from a directory server 240–241, 244
 - inheritance 247
 - organizing 238
 - search for 255

H

- hack tools 413
- Hardware Devices list
 - adding a device 568
 - using with device control 569
- hardware devices list 566
- health state
 - viewing 167
- Host Integrity
 - explained 571
 - requirements 574
 - setting up 572

- Host Integrity policies
 - notifications 580
 - peer-to-peer authentication 582
 - postpone Host Integrity check 577
 - Quarantine 581
 - remediation 576, 579
 - requirements 576
 - custom 583–584, 587–589
 - predefined 575
 - templates 583
 - settings 579
 - testing 589
- host triggers
 - firewall rules 360
- hosts
 - excluding from intrusion prevention 389

I

- icons
 - shield 169
- importing
 - firewall rules 369
 - Host Integrity Policy requirements
 - templates and 583
 - organizational units 244
 - policies 326
- index.ini
 - automatic update of whitelists and blacklists 554
 - creating file 556
- infected computers
 - identifying 403
 - rescanning 404
- inheritance 281
 - enabling 247
 - firewall rules 352, 354
- Insight 417, 436
 - modifying settings 474
- Insight Lookup
 - feature dependencies 437
- installation
 - client firewalls 113
 - client through Active Directory 799
 - communications ports 113
 - embedded database 65
 - internationalization 59
 - Microsoft SQL Server configuration settings 68
 - MSI command line examples 798
 - MSI Windows Security Center properties 796
 - planning 64

- installation *(continued)*
 - third-party software 789
 - through Active Directory Group Policy Object 799
 - using msi commands 791
- installation status 600
- installing
 - clients 118, 120, 122
- Intelligent Updater 227
- Internet bots 413
- Internet Browser Protection 475
- interoperability
 - of policy features 437
- intrusion prevention 380
 - blocking attacking computers 345
 - disabling on specified computers 389
 - enabling or disabling in Intrusion Prevention policy 386
 - how it works 383
 - locking and unlocking settings 330
 - managing custom signatures 391
 - notifications 390
 - platform comparison 784
 - signatures 384
 - testing custom signatures 397
- IPS signatures
 - custom
 - assigning libraries to a group 395
 - changing the order 395
 - libraries 395
 - regular expressions 816
 - variables 396
 - custom library 392
 - exceptions for 387

J

- JKS keystore file 687
- joke programs 413

L

- LDAP directory servers
 - connecting to 242
 - importing organizational units 244
- LDAP servers
 - importing user information from 240–241
- learned applications 356
 - about 331
 - enabling 332
 - searching for 333

- license
 - about 92
 - activating 96
 - additional 96
 - backing up 103
 - checking status 101
 - deployed 101
 - expired 101
 - over-deployed 101
 - purchasing 95
 - renewed 96
 - renewing 101
 - requirements 61
 - Symantec Licensing Portal 100
- license issues
 - notifications for 622
- limited administrator 293
 - configuring access rights 296
- Linux client
 - features 775
 - installing 132
 - management features 776
 - protection features 775
- LiveUpdate 181
 - about 182
 - and replication 729
 - checking server activity 194
 - client proxy settings for internal LiveUpdate server 195
 - configuring a site to download updates 189
 - configuring an external LiveUpdate server 196, 210
 - configuring an internal LiveUpdate server 211
 - configuring server download frequency 192
 - configuring update content for clients 196
 - content revisions 190
 - downloading to server 193
 - Group Update Provider 215, 223
 - Intelligent Updater 227
 - LiveUpdate Administrator 182
 - Mac 182
 - platform comparison 785
 - policies
 - configuring 196, 210–211
 - signatures and definitions 197
 - types of updates 197
 - updating definitions and content 197
 - updating whitelists and blacklists 557
 - using third-party distribution tools instead of 228

- LiveUpdate *(continued)*
 - whitelists and blacklists for system lockdown 554
- load balancing
 - defined 713
 - management server list 715
- local subnet traffic 374
- locations
 - associated with DNS queries 363
- locking
 - administrator account 84
- log on banner
 - adding 82
- log on screen
 - timing out 85
- logs 614
 - Apache 748
 - application and device control 615
 - audit 615
 - checking the debug log on the client 751
 - checking the inbox logs 752
 - clearing from database 711
 - computer status 616
 - database errors 613
 - deleting configuration settings 618
 - exporting data 596
 - filtering 617
 - Network Threat Protection 616
 - past 24-hours filter 617
 - reducing space in database 686, 701
 - refreshing 613
 - remote access 618
 - replicating 618
 - replication 729
 - Risk 616
 - running commands from 261
 - saving filter configurations 617
 - Scan 616
 - server
 - configuring size 709
 - SONAR 491
 - System 617
 - TruScan proactive threat scans 491
 - types 614
 - viewing 613
 - viewing remotely 618
- lost password
 - reset 307

M

- Mac client
 - features 775
 - installing 130
 - management features 776
 - protection features 775
- managed settings
 - configuring on client 267
- management server
 - uninstalling 77
- management server list
 - assigning to group and location 716
- management servers
 - sites 722
- Microsoft Active Directory
 - configuring templates 802
 - installing client software with Group Policy Object 799
- Microsoft Exchange server
 - automatic exclusions 415
- Microsoft SCCM/SMS
 - rolling out Package Definition Files 798
- Microsoft SQL Server
 - database configuration settings 68
- misleading applications 414
- mixed control 269
 - configuring Network Threat Protection settings 344
- MSI
 - Command line examples 798
 - features and properties 790
 - installing using command-line parameters 791
 - processing precedence with setaid.ini 791
- My Company group 236

N

- NetBIOS 343
- network adapters
 - adding to a rule 378
 - adding to default list 366
 - triggers 365
- network application monitoring 358
- network architecture 64
- network intrusion prevention
 - about 383
- network services
 - triggers 364
- Network Threat Protection
 - configuring for mixed control 344

Network Threat Protection *(continued)*

- creating notifications 390
- enabling or disabling 258
- logs 616
- platform comparison 784

notification area icon

- about 169

notifications

- about 620–621
- acknowledging 628
- creating 630
- default 622
- Do not show this message again 322
- filtering 630
- Host Integrity 580
- licensing 627
- Network Threat Protection 390
- partner 627
- preconfigured 622
- remote clients 288
- upgrades from another version 632
- virus and spyware events on client computers 450

O

on-demand scans

- running 426
- scan progress options 481

OS fingerprint masquerading 347

overview

- replication 722
- sites 722
- sites and replication 718

P

parental control programs 414

password

- .jks keystore file 688
- change 305
- resetting 306

Password never expires option 297

password protection

- client 273

passwords

- expiring 308
- resetting 307
- saving 82

peer-to-peer authentication 582

policies

- updating for remote clients 288

policy

- about 318
- Application and Device Control 318
- assign to a group 323
- creating 320
- editing 321
- Exceptions 318
- Firewall 318
- Host Integrity 318
- import and export 326
- inheritance 247
- Intrusion Prevention 318
- LiveUpdate 318
- non-shared 327
- shared 327
- user locks 330
- Virus and Spyware Protection 318
- withdraw 329

policy serial number

- viewing on the client 172

ports

- communication requirements 113
- installation requirements 113

Power Eraser

- about 763
- comparison to other scans 764
- differences between running locally and remotely 764
- responding to detections 772
- running a scan 770
- using to detect and remove difficult threats 766

print sharing 375

private Insight server 456

private server

- for groups 457

Proactive Threat Protection

- enabling or disabling 257

product

- components 50

protection

- enabling or disabling 256
- updating 181

proxy

- client external communication 444
- client submissions 444
- required exceptions when using authentication 434

proxy (*continued*)

- Symantec Endpoint Protection Manager connection to Symantec LiveUpdate 195

Q

Quarantine

- clean-up options 447
- deleting files 449
- Host Integrity failure 581
- local folder 446
- managing 445

quick reports

- creating 606

R

randomization

- content downloads 206–208

registry conditions

- Host Integrity custom requirement 586

regular expressions 816

- content arguments 827
- custom IPS signatures 818
- ICMP protocol arguments 822
- IP protocol arguments 823
- msg arguments 826
- sample IPS signature syntax 830
- streamdepth arguments 829
- TCP protocol arguments 819
- UDP protocol arguments 821

remediation

- Host Integrity 577, 579

remote access programs 414

remote clients

- monitoring 289
- policies for 286

remote consoles

- granting access 83

remote installation and TCP port 139 113

remote site 729

replication 729

- adding replication partner 730
- defined 722
- frequency 728
- on demand scheduling 727
- overview 718

replication partners

- deleting 729

report

- Comprehensive Risk 599
- Computers Not Scanned 598
- Daily Status 597
- favorite 597
- Infected and At Risk Computers 599
- New Risks Detected in the Network 599
- Top Sources of Attack 601
- Top Targets Attacked 601
- Top Traffic Notifications 601
- Weekly Status 597

reporting

- language 758
- logs 614
- SSL 758
- timestamps 758
- troubleshooting 758

reports

- deleting configuration settings 608
- overview 604
- printing 612
- saving 612
- saving configuration settings 608
- types 604

reputation data 436

Reset Copy Policy Reminder 322

restart

- avoiding 263
- command 261

risk

- reports 599

risk log 616

- deleting files from the Quarantine 449

risks

- remediating 401

rootkits 413

RSA server

- configuring SecurID authentication 298
- using with Symantec Endpoint Protection Manager 300

S

saving passwords

- logon screen 82

Scan log 616

scans 474

- about 408
- customizing administrator-defined 469
- managing 405

- scans (*continued*)
 - miscellaneous settings 475
 - Linux 476
 - paused 481
 - rescanning computers 404
 - Risk log events 475
 - Linux 476
 - running on demand 426
 - scan progress options 481
 - snoozed 481
 - stopped 481
- schedule
 - automatic database backup 702
- scheduled reports
 - creating 609
 - modifying 609
- scheduled scans
 - adding to a policy 422, 424–425
 - Mac clients 424–425
 - missed scans 423
 - multiple 423
 - saving as template 405
 - scan progress options 481
- screen reader
 - application blocked by Tamper Protection 502
- search for
 - groups, users, and computers 255
- SecurID authentication
 - configuring on the management server 298
- security assessment tool 414
- security risks
 - detections of 421
- Security Virtual Appliance 635, 655, 657
 - installation settings file 658
 - installing 654, 662
 - Shared Insight Cache service 665
 - uninstalling 670
 - using a script file to install 662
- serial number. *See* policy serial number
- server
 - configuring 76
 - connecting to 169
 - connecting to a directory server 242
 - heartbeat 169
 - logs 709
 - management 692
 - uninstalling 77
- server control 268
- servers
 - using a private Insight server 456
- setaid.ini
 - configuring 791
 - processing precedence with MSI features and properties 791
- settings
 - firewall 338, 347
 - Network Threat Protection 344
- share files and printers 375
- Shared Insight Cache 635, 637
 - network-based 639
 - cache results, issues 651
 - configuring network clients 643
 - customizing settings 644
 - installing 641
 - log 648
 - no result response 651
 - performance counters 650
 - stopping and starting the service 648
 - system requirements 640
 - uninstalling 641
 - viewing events 648
 - vShield-enabled 653, 657
 - configuration file 666
 - enabling 665
- shield icon 169
- sites
 - defined 722
 - overview 718
- smc command 806, 810
- SONAR
 - about 484
 - about detections 485
 - adjusting settings 490
 - exceptions for code injection 485, 498
 - false positives 488
 - feature dependencies 437
 - managing 486
 - monitoring scan events 491
- spyware 414
- stateful inspection 355
- status
 - client deployment 600
 - clients and computers 253
- status icon. *See* client connection
- stealth settings 347
- Submissions
 - locking and unlocking settings 330

- submissions 440–441
 - quarantined items 448
- symlink.xml
 - converting an unmanaged client to a managed client 173, 803
- Symantec Endpoint Protection
 - about 29
- Symantec Endpoint Protection clients
 - MSI features 793
 - MSI properties 792
- Symantec Insight for Private Clouds 456
- Symantec Licensing Portal. *See* license
- Symantec products
 - automatic exclusions 416
- Symantec Security Response 403
 - submissions 441
- system administrator 293
- system lockdown 542
 - about 523
 - application name list 553
 - checking the status of automatic updates 558
 - enabling whitelist mode 561
 - interaction with ATP: Endpoint 552
 - running in blacklist mode 562
 - running in test mode 559
 - testing selected items 564
- system log 617
- system requirements
 - network-based Shared Insight Cache 640
- system tray icon 169

T

- Tamper Protection
 - about 493
 - changing settings 494
 - locking and unlocking settings 330
 - when to disable 258
- TCP resequencing 347
- templates for scheduled scans 405
- terminated process errors
 - database 760
- third-party content distribution
 - about 228
 - enabling with a LiveUpdate Policy 229
 - to managed clients 229
 - Windows registry key requirement for unmanaged 230
- third-party software
 - installing client software 789

- threats
 - blended 413
- timeout parameters
 - console 85
 - database 759
- token traffic ring 343
- trackware 414
- trial
 - license 61
- trialware
 - license 96, 101
- Trojan horses 358, 413
- troubleshooting
 - client problems 748
 - network-based Shared Insight Cache 651
 - SymHelp 744
 - User Account Control and GPO 801
- trusted Web domain
 - creating an exception for 508
- trusted Web domain exception
 - feature dependencies 437

U

- uninstalling
 - client software with Active Directory GPO 804
 - Linux client 139
 - Mac client 138
 - management server 77
 - Security Software Removal 127
 - Windows client 137
- unlocking
 - administrator account 84
- unmanaged clients
 - distributing updates with third-party tools 230
- update
 - client 160
 - definitions 181
- user information
 - collect 272
- user interface
 - about 266
 - configuring 267, 270
- users
 - search for 255

V

- variables in signatures 396

- Virtual Image Exception tool 635, 673
 - running 673
 - system requirements 672
 - using on a base image 671
 - virtual images
 - exceptions 475
 - virtual machine
 - adjusting scans for 427
 - randomizing simultaneous content
 - downloads 206
 - virtualization 635, 637
 - adjusting scans for 427
 - base image for non-persistent GVMs 676
 - network-based Shared Insight Cache 643
 - randomizing scans 473
 - Security Virtual Appliance 655, 657
 - supported 62
 - Virtual Image Exception tool 671, 673
 - vShield-enabled Shared Insight Cache 665
 - Virus and Spyware Protection
 - platform comparison 781
 - preventing attacks 399
 - Virus and Spyware Protection policy
 - locking and unlocking settings 330
 - scheduled scans 422
 - virus definitions
 - updating 181
 - viruses 413
 - detections of 421
- ## W
- whitelist
 - updating automatically 554, 558
 - updating for system lockdown 557
 - whitelist mode
 - running system lockdown in 561
 - Windows 8
 - detections in 422
 - notifications 452
 - pop-up notifications 453
 - Windows client
 - features 775
 - management features 776
 - protection features 775
 - user mode and computer mode 263
 - Windows Embedded client
 - client installation package 114
 - Windows Installer
 - commands 791
 - Windows Installer *(continued)*
 - features and properties 790
 - parameters 795
 - Windows Security Center 475, 482
 - WINS traffic 343
 - withdrawing a policy 329
 - worms 413