

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



# Symantec™ Endpoint Protection and Symantec Network Access Control

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

Documentation version 11.00.02.01.00

## Legal Notice

Copyright © 2008 Symantec Corporation. All rights reserved.

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

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

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

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

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

Symantec Corporation  
20330 Stevens Creek Blvd.  
Cupertino, CA 95014

<http://www.symantec.com>

# Technical Support

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

Symantec's maintenance offerings include the following:

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

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

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

## Contacting Technical Support

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

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

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

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

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

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

## Licensing and registration

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

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

## Customer service

Customer service information is available at the following URL:

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

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

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

## Maintenance agreement resources

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

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

## Additional enterprise services

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

Enterprise services that are available include the following:

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

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

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

Select your country or language from the site index.

# Contents

Technical Support .....	4
Section 1     Basic administrative tasks .....	25
Chapter 1     Symantec Endpoint Protection Manager overview .....	27
About administrative tasks .....	27
Logging on to the Symantec Endpoint Protection Manager .....	29
How the Symantec Endpoint Protection Manager Console is organized .....	31
The Home page .....	34
The Monitors page .....	35
The Reports page .....	36
The Policies page .....	36
The Clients page .....	37
The Admin page .....	40
Chapter 2     Introduction to basic protection .....	43
Categories of protection .....	43
About Antivirus and Antispyware Protection .....	44
About Network Threat Protection .....	45
About Proactive Threat Protection .....	46
About Host Integrity and endpoint policy compliance .....	46
Chapter 3     Setting up domains, groups, and clients .....	49
About your security topology .....	50
About your group structure .....	50
About domains .....	51
About groups .....	51
About clients .....	53
About importing the organizational structure .....	54
Adding a domain .....	55
Administering a domain .....	56
Adding a group .....	56

	Deleting a group .....	56
	Renaming a group .....	57
	Moving a group .....	57
	Viewing a group's properties .....	58
	Adding clients as users .....	58
	Adding clients as computers .....	59
	Switching the client between user-based mode and computer-based mode .....	60
	Blocking clients from being added to groups .....	61
	Moving clients between groups .....	62
	Deleting clients .....	62
	Viewing a client's properties .....	63
	Searching for clients .....	64
	Filtering the list of clients .....	65
Chapter 4	Managing administrators .....	67
	About administrators .....	67
	About managing administrators .....	68
	Adding an administrator .....	69
	Switching between a non-limited and a limited administrator and configuring access rights .....	71
	Locking an administrator's account after too many logon attempts .....	72
	Authenticating administrators .....	73
	Renaming an administrator .....	73
	Changing an administrator's password .....	74
	Removing an administrator .....	74
Chapter 5	Working with client installation packages .....	77
	About client installation packages .....	77
	Configuring client installation package options .....	78
	Configuring installation package features .....	78
	Configuring client installation package settings .....	79
	Collecting user information .....	79
	Exporting client installation packages .....	80
	Adding client installation package updates and upgrading clients .....	81
	Adding client installation package updates .....	82
	Upgrading clients in one or more groups .....	83
	Deleting upgrade packages .....	84



Chapter 6	Updating definitions and content .....	85
	About LiveUpdate and updating definitions and content .....	85
	About update network distribution architectures .....	86
	About update types .....	89
	Configuring a site to download updates .....	89
	Configuring LiveUpdate Policies .....	92
	Configuring a LiveUpdate Settings Policy .....	92
	Configuring a LiveUpdate Content Policy .....	93
	Viewing and changing the LiveUpdate Content Policy that is applied to a group .....	95
	Configuring a Group Update Provider in a LiveUpdate Settings Policy .....	95
	Advanced update distribution options .....	96
	Providing antivirus content updates with Intelligent Updater .....	97
	About using third party distribution tools to distribute updates to managed clients .....	97
	Enabling third party content distribution to managed clients with a LiveUpdate Policy .....	98
	Distributing content to managed clients with third party distribution tools .....	99
	About using third party distribution tools to distribute updates to unmanaged clients .....	101
Chapter 7	Limiting user access to client features .....	103
	About access to the client interface .....	103
	Locking and unlocking managed settings .....	104
	Changing the user control level .....	105
	About mixed control .....	107
	Configuring user interface settings .....	108
	Password-protecting the client .....	109
Chapter 8	Setting up connections between management servers and clients .....	111
	About management servers .....	112
	Specifying a management server list .....	112
	Adding a management server list .....	113
	Assigning a management server list to a group and location .....	114
	Viewing the groups and locations to which a management server list is assigned .....	115

Editing the server name and description of a management server list .....	116
Editing the IP address, host name, and port number of a management server in a management server list .....	116
Changing the order in which management servers connect .....	117
Replacing a management server list .....	117
Copying and pasting a management server list .....	118
Exporting and importing a management server list .....	118
Deleting a management server list .....	119
About client and server communication settings .....	120

Chapter 9	Reporting basics .....	121
	About reporting .....	122
	About the reports you can run .....	123
	About the display of logs and reports .....	125
	How reporting uses the database .....	125
	About logged events from your network .....	125
	About the logs you can monitor .....	125
	Accessing the reporting functions .....	126
	Associating localhost with the IP address when you have loopback addresses disabled .....	127
	About using SSL with the reporting functions .....	128
	Using the Symantec Endpoint Protection Home page .....	128
	Configuring the Favorite Reports on the Home page .....	134
	About using Security Response links .....	136
	Using the Symantec Network Access Control Home page .....	137
	Configuring reporting preferences .....	139
	About Home and Monitors display options .....	140
	Configuring security status thresholds .....	141
	Configuring logs and reports preferences .....	142
	About the client scan times used in reports and logs .....	142
	About using the Past 24 hours filter in reports and logs .....	143
	About using the filters that search for groups in reports and logs .....	143

Chapter 10	Viewing and configuring reports .....	145
	Viewing reports .....	145
	About viewing line charts in reports .....	146
	About viewing bar charts .....	147
	Viewing the reports in Asian languages .....	147
	About reports .....	148
	Important points about reporting .....	161
	Creating quick reports .....	162

	Saving and deleting saved report filters .....	166
	About duplicate filter names .....	167
	Printing and saving a copy of a report .....	167
	Creating and deleting scheduled reports .....	168
Chapter 11	Viewing and configuring logs and notifications .....	171
	About logs .....	171
	About log types, contents, and commands .....	172
	Using the Monitors Summary tab .....	177
	Viewing logs .....	180
	Displaying event details in logs .....	181
	Viewing logs from other sites .....	181
	Saving and deleting filters .....	182
	About duplicate filter names .....	183
	Basic filter settings for logs .....	184
	Advanced filter settings for logs .....	185
	Running commands and actions from logs .....	186
	About reducing the volume of events sent to the logs .....	189
	Exporting log data .....	189
	Exporting log data to a text file .....	189
	Exporting data to a Syslog server .....	191
	Exporting log data to a comma-delimited text file .....	192
	Using notifications .....	193
	Viewing and filtering administrator notification information .....	193
	Threshold guidelines for administrator notifications .....	194
	Creating administrator notifications .....	195
	About editing existing notifications .....	199
Chapter 12	Using Monitors and Reports to help secure your network .....	201
	About using Monitors and Reports to help secure your network .....	201
	About the information in the Application Control and Device Control reports and logs .....	202
	About the information in the Audit report and log .....	203
	About the information in the Compliance reports and logs .....	204
	About the information in the Computer Status reports and log .....	206
	About the information in the Network Threat Protection reports and logs .....	208
	About the information in the TruScan proactive threat scan reports and logs .....	210
	About the information in the Risk reports and log .....	211

	About the information in the Scan reports and log .....	212
	About the information in the System reports and logs .....	213
	About eliminating viruses and security risks .....	216
	Identifying the infected and at risk computers .....	216
	Changing an action and rescanning the identified computers .....	216
	Restarting the computers that need a restart to finish remediation .....	217
	Updating definitions and rescanning .....	218
	About investigating and cleaning the remaining risks .....	218
	Eliminating the suspicious events .....	219
	Finding the clients that are offline .....	219
<b>Section 2</b>	<b>Advanced administrative tasks .....</b>	<b>221</b>
<b>Chapter 13</b>	<b>Managing single and multiple company sites .....</b>	<b>223</b>
	About the management of sites .....	223
	What you can do at a site .....	224
	What you cannot do at a site .....	225
	About site replication across different company sites .....	225
	About optional Enforcers at a site .....	225
	About remote sites .....	225
	Editing site properties .....	226
	Backing up a site .....	227
	Deleting remote sites .....	228
<b>Chapter 14</b>	<b>Managing servers .....</b>	<b>229</b>
	About the management of servers .....	229
	About servers and third-party passwords .....	230
	Starting and stopping the Symantec Endpoint Protection Manager service .....	230
	Granting or denying access to remote Symantec Endpoint Protection Manager consoles .....	231
	Deleting selected servers .....	232
	Exporting and importing server settings .....	233
<b>Chapter 15</b>	<b>Managing directory servers .....</b>	<b>235</b>
	About the management of directory servers .....	235
	Adding directory servers .....	235
	Synchronizing user accounts between directory servers and a Symantec Endpoint Protection Manager .....	237

	Importing information about users from an LDAP directory server .....	237
	Searching for users on an LDAP directory server .....	238
	Importing users from an LDAP directory server search results list .....	240
	About organizational units and the LDAP server .....	241
	Importing organizational units from an active or LDAP directory server .....	241
	Synchronizing organizational units .....	242
Chapter 16	Managing email servers .....	243
	About managing email servers .....	243
	Establishing communication between Symantec Endpoint Protection Manager and email servers .....	243
Chapter 17	Managing proxy servers .....	245
	About proxy servers .....	245
	Setting up a connection between an HTTP proxy server and the Symantec Endpoint Protection Manager .....	245
	Setting up a connection between an FTP proxy server and the Symantec Endpoint Protection Manager .....	246
Chapter 18	Managing RSA servers .....	249
	About prerequisites for using RSA SecurID with the Symantec Endpoint Protection Manager .....	249
	Configuring the Symantec Endpoint Protection Manager to use RSA SecurID Authentication .....	250
	Specifying SecurID Authentication for a Symantec Endpoint Protection Manager administrator .....	251
	Configuring the management server to support HTTPS communication .....	252
Chapter 19	Managing server certificates .....	253
	About server certificate types .....	253
	Updating a server certificate with a wizard .....	254
	Backing up a server certificate .....	256
	Locating the keystore password .....	257
Chapter 20	Managing databases .....	259
	About the management of databases .....	259
	About the naming conventions of a database .....	260

Management Server Configuration Wizard and Symantec Database Tools .....	260
About the backup and restoration of a database .....	261
About the reconfiguration of a database .....	262
About the scheduling of a database backup .....	263
Backing up a Microsoft SQL database .....	263
Backing up a Microsoft SQL database on demand from the Symantec Endpoint Protection Manager console .....	264
Backing up a Microsoft SQL database with the Database Maintenance Plan wizard .....	265
Backing up an embedded database on demand from the Symantec Endpoint Protection Manager .....	268
Scheduling automatic database backups from the Symantec Endpoint Protection Manager .....	269
Restoring a database .....	270
Editing the name and description of a database in the Symantec Endpoint Protection Manager console .....	271
Reconfiguring a database .....	272
Reconfiguring a Microsoft SQL database .....	272
Reconfiguring an embedded database .....	274
About managing log data .....	275
About log data and storage .....	275
Sweeping log data from the database manually .....	277
Log data from legacy clients .....	277
Configuring log settings for the servers in a site .....	277
About configuring event aggregation .....	278
Configuring client log settings .....	279
About configuring client log handling options for antivirus and antispymware policies .....	280
Backing up the logs for a site .....	280
About uploading large amounts of client log data .....	281
About managing log events in the database .....	282
Configuring database maintenance options for logs .....	283
About using the Interactive SQL utility with the embedded database .....	284
Changing timeout parameters .....	284
About recovering a corrupted client System Log on 64-bit computers .....	284
 Chapter 21	
Replicating data .....	287
About the replication of data .....	287
Understanding the impact of replication .....	290

	What settings are replicated .....	290
	How changes are merged during replication .....	291
	Setting up data replication .....	292
	Adding replication partners and schedule .....	292
	Scheduling automatic and on-demand replication .....	294
	Replicating data on demand .....	294
	Changing replication frequencies .....	295
	Replicating client packages .....	295
	Replicating logs .....	296
Chapter 22	Managing Tamper Protection .....	297
	About Tamper Protection .....	297
	Configuring Tamper Protection .....	298
Section 3	General policy management tasks .....	301
Chapter 23	About policies .....	303
	Overview of policies .....	303
	About shared and non-shared policies .....	305
	About policy-related tasks .....	306
	Groups, inheritance, locations, and policies .....	308
	Examples of policies .....	308
Chapter 24	Managing a group's inheritance for locations and policies .....	309
	About groups inheriting locations and policies from other groups .....	309
	Disabling and enabling a group's inheritance .....	310
Chapter 25	Managing a group's locations .....	311
	About a group's locations .....	311
	About locations and location awareness .....	312
	About planning locations .....	312
	About a group's default location .....	313
	Enabling a client's automatic assignment of policies .....	314
	Adding a location with a wizard .....	315
	Adding a location without a wizard .....	316
	Assigning a default location .....	317
	Editing the name and description of a group's location .....	318
	Deleting a group's location .....	318

Chapter 26	Working with policies .....	321
	About working with policies .....	322
	About adding policies .....	322
	Adding a shared policy in the Policies page .....	323
	Adding a non-shared policy in the Clients page with a wizard .....	324
	Adding a new non-shared policy in the Clients page .....	326
	Adding a new non-shared policy from an existing policy in the Clients page .....	326
	Adding a new non-shared policy from a previously exported policy file in the Clients page .....	327
	About editing policies .....	327
	Editing a shared policy in the Policies page .....	327
	Editing a non-shared or shared policy in the Clients page .....	328
	Assigning a shared policy .....	329
	Withdrawing a policy .....	330
	Deleting a policy .....	331
	Exporting a policy .....	332
	Importing a policy .....	333
	About copying policies .....	334
	Copying a shared policy in the Policy page .....	334
	Copying a shared or non-shared policy in the Clients page .....	335
	Pasting a policy .....	335
	Replacing a policy .....	336
	Converting a shared policy to a non-shared policy .....	337
	Converting a copy of a shared policy to a non-shared policy .....	338
Chapter 27	Pushing and pulling policies between management servers, clients, and optional Enforcers .....	339
	About pull mode and push mode .....	339
	About the heartbeat .....	340
	Specifying push or pull mode .....	340
Chapter 28	Setting up learned applications .....	343
	About learned applications .....	343
	Enabling learned applications .....	344
	Searching for applications .....	346
	Saving the results of an application search .....	347



Section 4	Configuring Antivirus and Antispyware Protection .....	349
Chapter 29	Basic Antivirus and Antispyware Policy settings .....	351
	Basics of Antivirus and Antispyware Protection .....	352
	About creating a plan to respond to viruses and security risks .....	352
	About viewing the antivirus and antispyware status of your network .....	354
	About running commands for Antivirus and Antispyware Protection .....	355
	About Antivirus and Antispyware Policies .....	355
	About working with Antivirus and Antispyware Policies .....	359
	About viruses and security risks .....	359
	About scanning .....	363
	About Auto-Protect scans .....	363
	About administrator-defined scans .....	367
	About TruScan proactive threat scans .....	369
	About scanning after updating definitions files .....	370
	About scanning selected extensions or folders .....	370
	About excluding named files and folders .....	373
	About actions for the viruses and the security risks that scans detect .....	374
	Setting up log handling parameters in an Antivirus and Antispyware Policy .....	375
	About client interaction with antivirus and antispyware options .....	376
	Changing the password that is required to scan mapped network drives .....	376
	Specifying how Windows Security Center interacts with the Symantec Endpoint Protection client .....	377
	Configuring the Symantec Endpoint Protection client to disable Windows Security Center .....	377
	Configuring Symantec Endpoint Protection alerts to appear on the host computer .....	378
	Configuring the out-of-date time for definitions .....	378
	Displaying a warning when definitions are out of date or missing .....	379
	Specifying a URL to appear in antivirus and antispyware error notifications .....	380
	Specifying a URL for a browser home page .....	381
	Configuring the options that apply to antivirus and antispyware scans .....	381

Configuring scans of selected file extensions .....	381
Configuring the scans of selected folders .....	382
About exceptions for security risks .....	383
Configuring actions for known virus and security risk detections .....	384
About notification messages on infected computers .....	385
Customizing and displaying notifications on infected computers .....	385
Submitting information about scans to Symantec .....	387
About submissions throttling .....	388
Configuring submissions options .....	389
Managing quarantined files .....	390
About Quarantine settings .....	390
Specifying a local Quarantine directory .....	390
Configuring automatic clean-up options .....	391
Submitting quarantined items to a central Quarantine Server .....	392
Submitting quarantined items to Symantec .....	393
Configuring actions to take when new definitions arrive .....	393
 Chapter 30	
Configuring Auto-Protect .....	395
About configuring Auto-Protect .....	395
About types of Auto-Protect .....	396
Enabling File System Auto-Protect .....	396
Configuring File System Auto-Protect .....	397
About Auto-Protect security risk scanning and blocking .....	398
Configuring advanced scanning and monitoring options .....	399
About Risk Tracer .....	399
Configuring Internet Email Auto-Protect .....	401
Configuring Microsoft Outlook Auto-Protect .....	402
Configuring Lotus Notes Auto-Protect .....	403
Configuring notification options for Auto-Protect .....	404
Displaying Auto-Protect results on infected computers .....	406
Adding warnings to infected email messages .....	406
Notifying senders of infected email messages .....	407
Notifying others of infected email messages .....	408
Configuring progress notifications for Auto-Protect scans of Internet email .....	410
 Chapter 31	
Using administrator-defined scans .....	411
About using administrator-defined scans .....	411
Adding scheduled scans to an Antivirus and Antispyware Policy .....	412

	Setting options for missed scheduled scans .....	413
	Editing, deleting, or disabling scheduled scans .....	414
	Configuring on-demand scan options .....	415
	Running on-demand scans .....	416
	Configuring scan progress options for administrator-defined scans .....	418
	Setting advanced options for administrator-defined scans .....	419
Section 5	Configuring Network Threat Protection .....	421
Chapter 32	Basic Network Threat Protection settings .....	423
	About Network Threat Protection and network attacks .....	424
	How Symantec Endpoint Protection protects computers against network attacks .....	424
	About the firewall .....	425
	About working with Firewall Policies .....	426
	About firewall rules .....	427
	About the elements of a firewall rule .....	427
	About the rule processing order .....	432
	About stateful inspection .....	435
	Adding blank rules .....	436
	Adding rules with the Add Firewall Rule Wizard .....	438
	Adding inherited rules from a parent group .....	439
	Importing and exporting rules .....	440
	Editing and deleting rules .....	441
	Copying and pasting rules .....	442
	Changing the order of rules .....	442
	Enabling and disabling rules .....	443
	Enabling Smart traffic filtering .....	443
	Enabling traffic and stealth settings .....	444
	Configuring peer-to-peer authentication .....	445
Chapter 33	Configuring intrusion prevention .....	447
	About the intrusion prevention system .....	447
	About the Symantec IPS signatures .....	448
	About custom IPS signatures .....	448
	Configuring intrusion prevention .....	449
	About working with Intrusion Prevention Policies .....	450
	Enabling intrusion prevention settings .....	450
	Changing the behavior of Symantec IPS signatures .....	451
	Blocking an attacking computer .....	452

	Setting up a list of excluded computers .....	453
	Creating custom IPS signatures .....	454
	Assigning multiple custom IPS libraries to a group .....	456
	Changing the order of signatures .....	457
	Copying and pasting signatures .....	457
	Defining variables for signatures .....	458
Chapter 34	Customizing Network Threat Protection .....	461
	Enabling and disabling Network Threat Protection .....	462
	Configuring Network Threat Protection settings for mixed control .....	463
	Adding hosts and host groups .....	464
	Editing and deleting host groups .....	464
	Adding hosts and host groups to a rule .....	465
	Adding network services .....	466
	Editing and deleting custom network services .....	467
	Adding network services to a rule .....	468
	Enabling network file and printer sharing .....	469
	Adding network adapters .....	470
	Adding network adapters to a rule .....	471
	Editing and deleting custom network adapters .....	472
	Adding applications to a rule .....	472
	Adding schedules to a rule .....	474
	Configuring notifications for Network Threat Protection .....	475
	Configuring email messages for traffic events .....	476
	Setting up network application monitoring .....	477
Section 6	Configuring Proactive Threat Protection .....	479
Chapter 35	Configuring TruScan proactive threat scans .....	481
	About TruScan proactive threat scans .....	481
	About using the Symantec default settings .....	482
	About the processes that TruScan proactive threat scans detect .....	483
	About managing false positives detected by TruScan proactive threat scans .....	484
	About the processes that TruScan proactive threat scans ignore .....	487
	How TruScan proactive threat scans work with Quarantine .....	488
	How TruScan proactive threat scans work with centralized exceptions .....	488
	Understanding TruScan proactive threat detections .....	490

	Specifying the types of processes that TruScan proactive threat scans detect .....	491
	Specifying the actions and sensitivity levels for detecting Trojan horses, worms, and keyloggers .....	491
	Specifying actions for commercial application detections .....	492
	Configuring the TruScan proactive threat scan frequency .....	493
	Configuring notifications for TruScan proactive threat scans .....	494
Chapter 36	Configuring Application and Device Control .....	495
	About application and device control .....	495
	About the structure of an Application and Device Control Policy .....	496
	About application control .....	497
	About Test mode .....	498
	About application control rule sets and rules .....	498
	About device control .....	501
	About working with Application and Device Control Policies .....	502
	Enabling a default application control rule set .....	503
	Creating an Application and Device Control Policy .....	504
	Configuring application control for an Application and Device Control Policy .....	504
	Creating a new application control rule set and adding a new rule to the set .....	505
	Adding conditions to a rule .....	506
	Configuring condition properties for a rule .....	507
	Configuring the actions to take when a condition is met .....	509
	Applying a rule to specific applications and excluding applications from a rule .....	510
	Changing the order in which application control rule sets are applied .....	511
	Disabling application control rule sets and individual rules in an Application and Device Control Policy .....	512
	Changing the mode of an application control rule set .....	513
	Configuring device control for an Application and Device Control Policy .....	513
Chapter 37	Setting up hardware devices .....	515
	About hardware devices .....	515
	About class IDs .....	516
	Obtaining a device ID from Control Panel .....	516
	Adding a hardware device .....	516
	Editing a hardware device .....	517
	Deleting a hardware device .....	517

Chapter 38	Customizing Application and Device Control Policies .....	519
	About authorizing the use of applications, patches, and utilities .....	519
	Creating and importing a file fingerprint list .....	520
	Creating a file fingerprint list .....	520
	Editing a file fingerprint list .....	522
	Importing a file fingerprint list into a shared policy .....	522
	Merging file fingerprint lists into a shared policy .....	523
	Deleting a file fingerprint list .....	524
	About system lockdown .....	524
	System lockdown prerequisites .....	525
	Setting up system lockdown .....	526
Section 7	Configuring centralized exceptions .....	529
Chapter 39	Configuring Centralized Exceptions Policies .....	531
	About Centralized Exceptions Policies .....	531
	About working with Centralized Exceptions Policies .....	532
	About centralized exceptions for antivirus and antispyware scans .....	532
	About centralized exceptions for TruScan proactive threat scans .....	533
	About centralized exceptions for Tamper Protection .....	533
	About client interaction with centralized exceptions .....	534
	Configuring a Centralized Exceptions Policy .....	534
	Configuring a centralized exception for antivirus and antispyware scans .....	535
	Configuring a centralized exception for TruScan proactive threat scans .....	537
	Configuring a centralized exception for Tamper Protection .....	539
	Configuring client restrictions for centralized exceptions .....	540
	Creating centralized exceptions from log events .....	540
	Adding a centralized exception for risk events .....	541
	Adding a centralized exception for TruScan proactive threat scan events .....	541
	Adding a centralized exception for Tamper Protection events .....	542

Section 8	Configuring Host Integrity for endpoint policy compliance .....	543
Chapter 40	Basic Host Integrity settings .....	545
	How Host Integrity enforcement works .....	545
	About working with Host Integrity Policies .....	548
	About the Quarantine Policy .....	548
	About Host Integrity requirement planning .....	548
	About Host Integrity requirements .....	549
	Adding Host Integrity requirements .....	550
	Editing and deleting a Host Integrity requirement .....	552
	Enabling and disabling Host Integrity requirements .....	552
	Changing the sequence of Host Integrity requirements .....	553
	Adding a Host Integrity requirement from a template .....	553
	About settings for Host Integrity checks .....	554
	Setting up logging and notifications for a Host Integrity check .....	555
	Allowing the Host Integrity check to pass if a requirement fails .....	556
	About Host Integrity remediation .....	557
	About restoring applications and files for Host Integrity .....	558
	Host Integrity remediation and Enforcer settings .....	558
	Specifying the amount of time the client waits to remediate .....	559
	Allowing users to postpone or cancel Host Integrity remediation .....	560
Chapter 41	Adding custom requirements .....	563
	About custom requirements .....	563
	About conditions .....	564
	About antivirus conditions .....	564
	About antispyware conditions .....	565
	About firewall conditions .....	565
	About file conditions .....	566
	About operating system conditions .....	568
	About registry conditions .....	568
	About functions .....	570
	About custom requirement logic .....	571
	About the RETURN statement .....	571
	About the IF, THEN, and ENDIF statement .....	571
	About the ELSE statement .....	572
	About the NOT keyword .....	572
	About AND, OR keywords .....	572

Writing a custom requirement script .....	573
Adding an IF THEN statement .....	574
Switching between the IF statement and the IF NOT statement .....	575
Adding an ELSE statement .....	575
Adding a comment .....	575
Copying and pasting IF statements, conditions, functions, and comments .....	576
Deleting a statement, condition, or function .....	576
Displaying a message dialog box .....	576
Downloading a file .....	577
Generating a log message .....	578
Running a program .....	578
Running a script .....	579
Setting the timestamp of a file .....	580
Specifying a wait time for the script .....	581
 Appendix A	
Using the command-line interface .....	583
The client service .....	583
Error codes .....	587
Typing a parameter if the client is password-protected .....	587
 Index .....	589



## Basic administrative tasks

- [Symantec Endpoint Protection Manager overview](#)
- [Introduction to basic protection](#)
- [Setting up domains, groups, and clients](#)
- [Managing administrators](#)
- [Working with client installation packages](#)
- [Updating definitions and content](#)
- [Limiting user access to client features](#)
- [Setting up connections between management servers and clients](#)
- [Reporting basics](#)
- [Viewing and configuring reports](#)
- [Viewing and configuring logs and notifications](#)
- [Using Monitors and Reports to help secure your network](#)



# Symantec Endpoint Protection Manager overview

This chapter includes the following topics:

- [About administrative tasks](#)
- [Logging on to the Symantec Endpoint Protection Manager](#)
- [How the Symantec Endpoint Protection Manager Console is organized](#)

## About administrative tasks

Before you perform administrative tasks in Symantec Endpoint Protection Manager, you must have installed the management server in a test environment. The system administrator who installs the management server performs the administration tasks for Symantec Endpoint Protection and Symantec Network Access Control.

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

Administrative tasks include basic and advanced administrative tasks. Most organizations need to perform only the basic administrative tasks. Smaller, less-complex organizations are less likely to perform the advanced administrative tasks. Most of the default settings should be sufficient for the requirements of the basic administrative tasks. These default settings are described first. Organizations that customize the default settings perform the advanced administrative tasks.

[Table 1-1](#) describes the organization of the document sections, who should read that section, and an overview of the contents.

**Table 1-1** Document organization and contents

Section	Audience
Section 1: Basic administrative tasks	For all administrators.  Includes managing the administrators, managing the clients, updating the definitions and the content, and the basics of reporting and monitoring.
Section 2: Advanced administrative tasks	For larger organizations.  Includes managing multiple sites, managing servers of various types, replicating data from one site to another, and managing Tamper Protection.
Section 3: General policy management tasks	For all administrators.  Includes an overview of policies of all types, the concepts of inheritance and locations, and using learned applications.
Section 4: Configuring Antivirus and Antispyware Protection	For all administrators.  Includes Antivirus and Antispyware Policy setting, configuring Auto-Protect, and setting up administrator-defined scans.
Section 5: Configuring Network Threat Protection	For administrators who need to configure firewalls.  Default settings are usually enough, but administrators who have a detailed understanding of networks can fine tune their settings.
Section 6: Configuring Proactive Threat Protection	For administrators who need to go beyond antivirus, antispyware, intrusion prevention, and firewall protection technologies.  Uses heuristics to detect unknown threats.
Section 7: Configuring centralized exceptions	For larger organizations.  Includes the information on how to set up exceptions for antivirus and antispyware scans, TruScan proactive threat scans, and Tamper Protection scans.

**Table 1-1** Document organization and contents (*continued*)

Section	Audience
Section 8: Configuring Host Integrity for endpoint policy compliance	Optional component. Describes how to set up Host Integrity Policies to ensure the compliance of endpoints with the security policy.
Appendix A: Using the command-line interface	For all administrators. Lists the client service parameters you can use with the <code>smc</code> command.

## Logging on to the Symantec Endpoint Protection Manager

You can log on to the Symantec Endpoint Protection Manager Console after you install Symantec Endpoint Protection. You can log on to the console in either of two ways. You can log on remotely, from another computer that meets the system requirements for a remote Console. You can also log on to the console locally, by using the computer on which Symantec Endpoint Protection Manager is installed.

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

What you can view and do from the console depends on the type of administrator you are. You can log on as a system administrator, an administrator, or a limited administrator. A system administrator has full privileges across all domains. An administrator has those privileges that are constrained to a specific domain. A limited administrator has a subset of the administrator privileges and is also constrained to a specific domain. If you installed Symantec Endpoint Protection Manager, you are a system administrator. If someone else installed the Manager, your status may be different. Most organizations, however, do not need to be concerned about domains or limited administrator status.

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

See [“About administrators”](#) on page 67.

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

- 1 Open a 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 Symantec Endpoint Protection Manager. By default, the Symantec Endpoint Protection Manager Console uses port number 9090, but you can change it if you run the Management Server Configuration wizard.

- 2 When you see the Symantec Endpoint Protection Manager Console Web page, click the link to display the logon screen.

The computer from which you log on must have the Java 2 Runtime Environment (JRE) installed. If it does not, you are prompted to download and install it. Follow the prompts to install the JRE.

The computer must also have Active X and scripting enabled.

- 3 When you log on, you may see a message that warns of a host name mismatch. If this message appears, in response to the prompt, click **Yes**.

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

- 4 In the Symantec Endpoint Protection Manager download window that appears, click the link to download the Symantec Endpoint Protection Manager.
- 5 Click **Yes** or **No** as desired when you are prompted to create desktop and start menu shortcuts.

Both are acceptable options.

- 6 In the Symantec Endpoint Protection Manager Console logon window that displays, type your user name and password. If this logon is your first Symantec Endpoint Protection logon after installation, type the account name: **admin**. Then, type the password that you configured when you installed the product.

- 7 If your network has only one domain, skip this step.

If your network has multiple domains, in the Domain text box, type the name of the domain to which you want to log on.

If the Domain text box is not visible, click **Options>>**. Whether the Domain text box is visible depends on its state the last time you logged on.

- 8 Click **Log On**.

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

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

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

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

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

- 3 Do one of the following tasks:

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

- 4 Click **Log on**.

## How the Symantec Endpoint Protection Manager Console is organized

The Symantec Endpoint Protection Manager Console provides an in-depth view of your network's security. It provides a central location from which to manage Symantec Endpoint Protection and Symantec Network Access Control. The console is where you make client security policy changes.

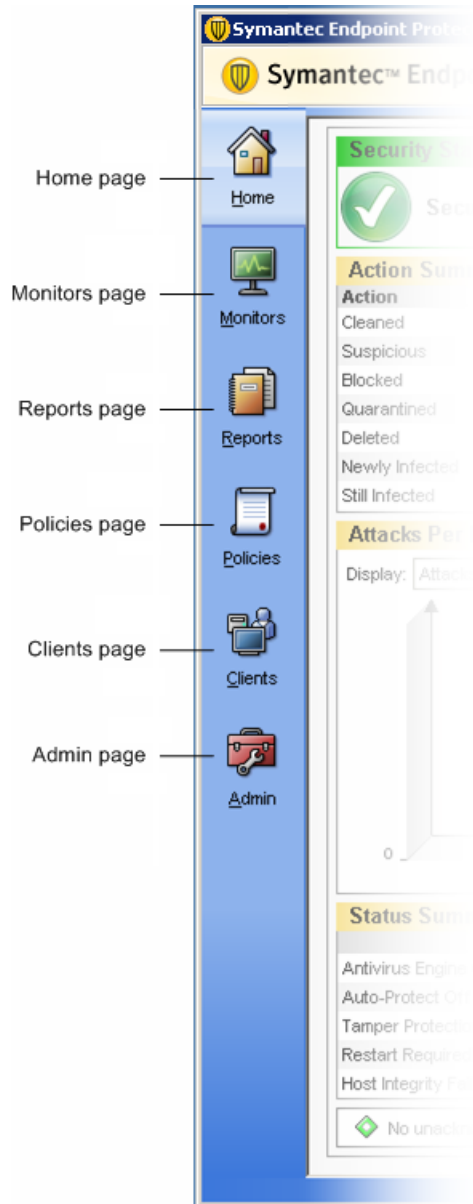
When you first log on to the Symantec Endpoint Protection Manager, you see the Symantec Endpoint Protection Manager Console Home page and a navigation bar that contains page tabs. The Symantec Endpoint Protection Manager Console navigation bar runs down the left-hand side of the pane. The Symantec Endpoint Protection Manager contains six pages. Each of the pages represents a major

management functional category. An icon represents each functional category, along with descriptive text about that page's function. You can click an icon in the navigation bar to display its corresponding page. The icons are always available to help you navigate from page to page.

[Figure 1-1](#) shows the Symantec Endpoint Protection Manager navigation bar.



Figure 1-1 Navigation bar



---

**Note:** System administrators and limited administrators may see fewer options, depending on the permissions that are assigned to their accounts.

---

The Home page, Monitors page, and Reports page provide the reporting functions that you use to monitor the security of your network. The Policies page, Clients page, and Admin page are used to configure and manage your network security policy.

Table 1-2 lists each navigation bar icon and describes the functionality to which it links.

Table 1-2 Navigation icons

Label	Description
Home	Displays the security status of your network and virus definition summary information. This page is your control panel and it is the default page to which the Symantec Endpoint Protection Manager Console opens.
Monitors	Displays the monitoring logs. You can also use these pages to view and configure notifications, and to monitor the status of commands.
Reports	Displays the reports. You have a choice of predefined and customizable Quick Reports and configurable Scheduled Reports.
Policies	Displays the policies for each policy type. Use this page to manage your policies.
Clients	Displays the policy information for clients and groups. Use this page to manage the policies that get pushed to the clients through installation packages.
Admin	Displays the administrator-specific configuration information.

## The Home page

The Home page displays general security status and virus definition summary information. If you have Symantec Endpoint Protection installed, then your Home page displays information about the security of your network. If you have only Symantec Network Access Control installed, then your Home page displays automatically generated reports about the compliance status of your network.

The Symantec Endpoint Protection Home page contains the following sections:

- Security Status
- Action Summary by Detection Count
- Attacks, Risks, or Infections per Hour: Past 12 Hours
- Status Summary, including the unacknowledged notifications in the last 24 hours

- Virus Definitions Distribution or Intrusion Prevention Signatures
- Security Response information and links
- Watched Applications Summary
- Favorite Reports

See [“Using the Symantec Endpoint Protection Home page”](#) on page 128.

The Symantec Network Access Control Home page contains the following sections:

- Failed Network Compliance Status
- Compliance Status Distribution
- Clients by Compliance Failure Summary
- Compliance Failure Details

See [“Using the Symantec Network Access Control Home page”](#) on page 137.

## Security Status

Security Status can be either Good or Attention Needed. If the status is Attention Needed, you can click the red X icon or the More Details link to view more information. You can also click Preferences to access the Preferences page where you can configure your reporting preferences.

See [“Configuring security status thresholds”](#) on page 141.

## Favorite Reports

By default, the Favorite Reports section of the Home page contains the following reports:

- Top Sources of Attack
- Top Risk Detections Correlation
- TruScan Proactive Threat Distribution

You can click the plus-sign icon to the right of Favorite Reports to change which reports appear in this section of the Home page.

See [“Configuring the Favorite Reports on the Home page”](#) on page 134.

## The Monitors page

You can use the Monitors page to display information from logs, to view and configure notifications, and to view command status. This page contains the logs and notifications that administrators can use to monitor their networks.

The Monitors page contains the following tabs:

- **Summary**

If you have Symantec Endpoint Protection installed, you have several summary views to choose from. You can select to view Antivirus and Antispyware Protection, Network Threat Protection, Compliance, or Site Status. If you have only Symantec Network Access Control installed, then the Summary tab displays the Site Status information. If you have only Symantec Network Access Control installed, the Compliance information appears on the Home page. See [“Using the Monitors Summary tab”](#) on page 177.

- **Logs**

The logs present the detailed information that is collected from your security products. Logs contain event data from both management servers and clients. You can also perform actions from some of the logs. Some administrators prefer to monitor their network primarily by using logs. See [“About log types, contents, and commands”](#) on page 172.

- **Command Status**

The Command Status tab displays the status of the commands that you have run from the Symantec Endpoint Protection Manager Console and their details. See [“Running commands and actions from logs”](#) on page 186.

- **Notifications**

A notification is a message that alerts you about potential security problems in your network. You can configure many different kinds of events to trigger a notification. The notifications on the Notifications tab are directed at administrators, not users. See [“Using notifications”](#) on page 193.

## The Reports page

You can use the Reports page to obtain broad overviews of the status of security in your network. Reports are graphical snapshots of the events that happen in your network and statistics about the events. You can use the filters on the Reports page to generate predefined or custom reports. The predefined reports are located on the Quick Reports tab. On the Scheduled Reports tab, you can schedule reports to run at regular intervals and have them sent by email to yourself or others.

See [“About reports”](#) on page 148.

## The Policies page

You can use the Policies page to create policies that are downloaded to the client. Clients connect to the server to get the latest policies and security settings, and

software updates are deployed from there. The policies that appear depend on the product components that you installed.

The Policies page contains the following panes:

- **View Policies**  
The View Policies pane lists the policy types that can be viewed in the upper right-hand pane: Antivirus and Antispyware, Firewall, Intrusion Prevention, Application and Device Control, LiveUpdate, and Centralized Exceptions. You can also view Host Integrity Policies if Symantec Network Access Control is installed. Click the arrow next to Policy Components to expand the list of components if it is not already displayed.
- **Policy Components**  
The Policy Components pane lists the various types of policy components that are available. These components include management server lists, file fingerprint lists, among others.
- **Tasks**  
The Tasks pane lists the appropriate tasks for the policy that you select under View Policies.
- ***Policy type* Policies pane**  
The right-hand pane changes in response to the policy that you select under View Policies. For some choices, the pane is split horizontally. In these cases, the bottom half of the pane shows the recent changes for the selected policy.

For information about the different types of policies and their options, see the chapters that describe the policies.

## The Clients page

You can use the Clients page to manage the computers and users in your network.

The Clients page contains the following panes:

- **View Clients**  
The View Clients page displays the groups in the client management structure, arranged hierarchically in a tree structure. By default this structure contains the Global group and under it, the Temporary group.
- **Tasks**  
The Tasks pane lists the client-related tasks that you can perform.
- ***group name* pane**  
The right pane contains four tabs: Clients, Policies, Details, and Install Packages. Each tab displays the content that pertains to the group that you selected in the View Clients pane.

You can perform the following tasks from the Clients tab:

- Add groups, computer accounts, and user accounts.
- Import an organizational unit or a container.
- Import users directly from the Active Directory or an LDAP server.
- Run commands on groups.
- Search for clients.
- Display groups or users.
- Search for unmanaged computers.

From the Policies tab, you can set some location-independent options for LiveUpdate content, client logs, communications, and some general settings. You can also set some location-specific options such as the control mode and either push or pull communication between the server and client. You can perform the following tasks from the Policies tab:

- Add locations.
- Manage locations.
- Copy group policies.
- Add groups.

You can perform the following tasks from the Details tab:

- Add groups.
- Import an organizational unit or a container.
- Delete groups.
- Rename groups.
- Move groups.
- Edit group properties.







From the Install Packages tab, you can configure and add a new client installation package. Use the management server to create and then export one or more client installation packages to a management server in the site. After you export the client installation package to the management server, you then install the files in the package on client computers.

## **About the client status icons**




When you view the clients in the groups, the icons appear next to the clients and indicate the status.

Table 1-3 illustrates and describes the icons.

**Table 1-3** Client status icons

Icon	Description
	This icon indicates the following status: <ul style="list-style-type: none"> <li>■ The client is communicating with Symantec Endpoint Protection Manager.</li> <li>■ The client is in computer mode.</li> </ul>
	This icon indicates the following status: <ul style="list-style-type: none"> <li>■ The client is not communicating with Symantec Endpoint Protection Manager.</li> <li>■ The client is in computer mode.</li> <li>■ The client may have been added from the console, and may not have any Symantec client software installed.</li> </ul>
	This icon indicates the following status: <ul style="list-style-type: none"> <li>■ The client is communicating with Symantec Endpoint Protection Manager.</li> <li>■ The client is in computer mode.</li> <li>■ The client is an unmanaged detector.</li> </ul>
	This icon indicates the following status: <ul style="list-style-type: none"> <li>■ The client is not communicating with Symantec Endpoint Protection Manager.</li> <li>■ The client is in computer mode.</li> <li>■ The client is an unmanaged detector.</li> </ul>
	This icon indicates the following status: <ul style="list-style-type: none"> <li>■ The client is communicating with Symantec Endpoint Protection Manager.</li> <li>■ The client is in user mode.</li> </ul>
	This icon indicates the following status: <ul style="list-style-type: none"> <li>■ The client is not communicating with Symantec Endpoint Protection Manager.</li> <li>■ The client is in user mode.</li> <li>■ The client may have been added from the console, and may not have any Symantec client software installed.</li> </ul>

**Table 1-3** Client status icons (*continued*)

Icon	Description
	<p>This icon indicates the following status:</p> <ul style="list-style-type: none"> <li>■ The client is communicating with Symantec Endpoint Protection Manager at another site.</li> <li>■ The client is in computer mode.</li> </ul>
	<p>This icon indicates the following status:</p> <ul style="list-style-type: none"> <li>■ The client is communicating with Symantec Endpoint Protection Manager at another site.</li> <li>■ The client is in computer mode.</li> <li>■ The client is an unmanaged detector.</li> </ul>
	<p>This icon indicates the following status:</p> <ul style="list-style-type: none"> <li>■ The client is communicating with Symantec Endpoint Protection Manager at another site.</li> <li>■ The client is in computer mode.</li> </ul>

The users on the client can also view similar status icons. For more information, see the *Client Guide for Symantec Endpoint Protection and Symantec Network Access Control*.

## The Admin page

You can use the Admin page to manage the administrator accounts, domain properties, server properties and site properties, and client installation packages for your network. When you select the Administrators tab, the View pane shows all administrators who manage the domain into which the administrator is logged. It includes all system administrators, administrators, and limited administrators. The Symantec Endpoint Protection Manager Admin page contains the following panes:

- View Administrators, Domains, Servers, or Install Packages.  
 The view that appears depends on the selection that you make at the bottom of the navigation pane.
- Tasks  
 The Tasks pane lists the tasks that you can perform from the Admin page. These tasks change based on the selection that you make at the bottom of the navigation pane.
- The right-hand pane



The right pane displays the content that pertains to the selection that you make at the bottom of the navigation pane.

When you select Administrators, you can add, delete, and edit administrator accounts.

When you select Domains, you can add, rename, and edit the properties of domains. Domains provide a logical way to group computers in large networks. If you have a small network, you probably use only the default domain, which is named Default.

When you select Servers, the tasks that are available change based on what you have selected in the View Servers navigation tree. You can select the Local Site, a specific server, or the local host.

When you select Local Site, you can perform the following tasks:

- Edit site properties, such as Console timeout period, LiveUpdate settings, and database settings.
- Configure external logging to send log data to a file server or a Syslog server.
- Add a partner for site replication.
- Download LiveUpdate content.
- Display LiveUpdate status.
- Display LiveUpdate downloads.

When you select a specific server, you can perform the following tasks:

- Edit server properties, such as the mail server, directory server, and proxy server options.
- Delete servers.
- Manage server authentication certificates.
- Configure RSA SecurID authentication.
- Import and export this server's properties as an XML file.

When you select Install Packages, you can add, delete, edit, and export client installation packages. You can also send a package to groups and you can set options for collecting user information.



# Introduction to basic protection

This chapter includes the following topics:

- [Categories of protection](#)

## Categories of protection

Symantec Endpoint Protection provides several categories of protection for the computers in your security network.

These categories include:

- Antivirus and Antispyware Protection
- Network Threat Protection
- Proactive Threat Protection
- Host Integrity

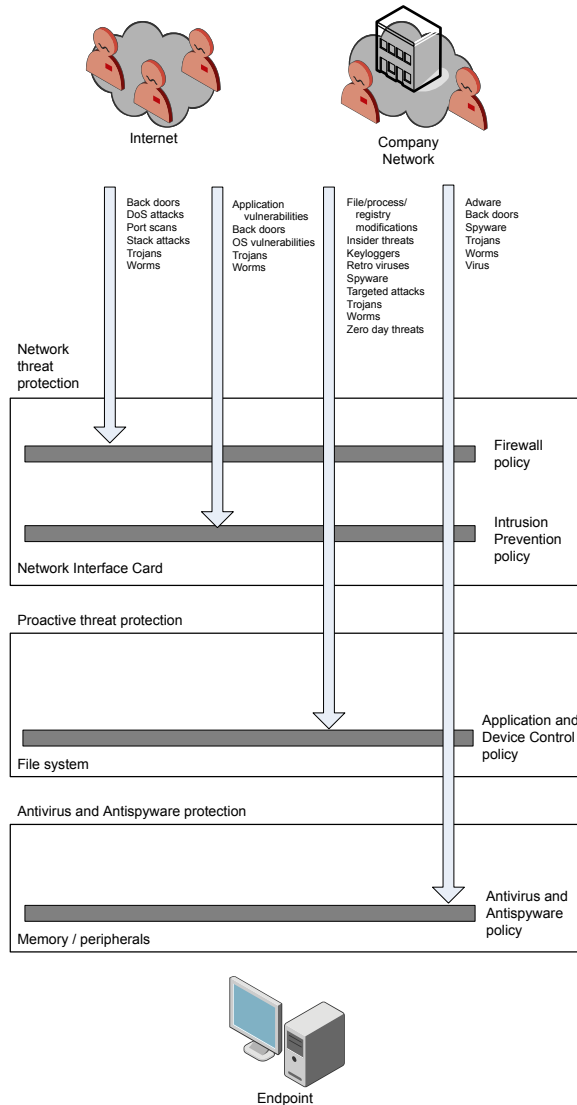
---

**Note:** Host Integrity Policies are available only with the Symantec Network Access Control product. Symantec Network Access Control can be installed alone, or can be installed with Symantec Endpoint Protection. All other categories of protection are standard with Symantec Endpoint Protection, and do not come with Symantec Network Access Control.

---

[Figure 2-1](#) shows the categories of threats that are blocked by each type of protection.

Figure 2-1 Protection layer overview



## About Antivirus and Antispyware Protection

Symantec Endpoint Protection Antivirus and Antispyware Protection provides protection from viruses and security risks, and in many cases can repair their side effects. The protection includes real-time scanning of files and email as well as scheduled scans and on-demand scans. Antivirus and antispyware scans detect

both viruses and security risks, such as spyware, adware, and other files that can put a computer, as well as a network, at risk.

The scans also detect kernel-level rootkits. Rootkits are programs that try to hide themselves from a computer's operating system and could be used for malicious purposes.

You can apply the default Antivirus and Antispyware Policy to client computers in your network. You can create additional Antivirus and Antispyware Policies and apply them as needed. You can edit the policy when requirements in your security network change.

The default Antivirus and Antispyware Policy is designed to be appropriate for companies of all sizes. It provides strong protection while minimizing impact to endpoint resources.

See [“Basics of Antivirus and Antispyware Protection”](#) on page 352.

## About Network Threat Protection

Network Threat Protection provides a firewall and intrusion prevention protection to prevent intrusion attacks and malicious content from reaching the computer that runs the Symantec Endpoint Protection client. The firewall allows or blocks network traffic based on various criteria that the administrator or end user sets.

Firewall rules determine whether an endpoint allows or blocks an incoming or outgoing application or service from gaining access through its network connection. Firewall rules allow the client to systematically allow or block incoming or outgoing applications and traffic from or to specific IP addresses and ports. Security settings detect and identify common attacks, send email messages after an attack, display customizable messages, and perform other related security tasks.

The client also analyzes all the incoming and the outgoing information for the data patterns that are typical of an attack. It detects and blocks malicious traffic and attempts by outside users to attack the client computer. Intrusion prevention also monitors outbound traffic and prevents the spread of worms.

The default Network Threat Protection Policy is designed to be appropriate for companies of all sizes. It provides strong protection while minimizing impact to endpoint resources. You can edit the default policy or create new policies and apply them to the endpoints on your network.

See [“About Network Threat Protection and network attacks”](#) on page 424.

## About Proactive Threat Protection

Proactive Threat Protection provides protection against zero-day attack vulnerabilities in your network. Zero-day attack vulnerabilities are new vulnerabilities that are not yet publicly known. Threats that exploit these vulnerabilities can evade signature-based detection (such as antispyware and antispyware definitions). Zero-day attacks may be used in targeted attacks and in the propagation of malicious code.

Proactive Threat Protection includes the following:

- TruScan proactive threat scans
- Application and Device Control Policies

The default settings for Proactive Threat Protection are designed to be appropriate for companies of all sizes. You can edit those settings and create new ones as your needs change.

Proactive threat scanning uses heuristics to flag potentially harmful processes and applications. Heuristics look at the behavior of processes on a client computer. For example, opening a port.

See [“About TruScan proactive threat scans”](#) on page 481.

Application and Device Control Policies provide a way to block or limit processes or hardware devices on client computers.

See [“About application and device control”](#) on page 495.

## About Host Integrity and endpoint policy compliance

Host Integrity gives you the ability to define, enforce, and restore the security of clients to secure enterprise networks and data. You set up Host Integrity Policies to verify that clients attempting network access are running antivirus software, patches, and hotfixes and other application criteria. You set up Host Integrity Policies to run on client computers at startup and periodically afterward.

See [“How Host Integrity enforcement works”](#) on page 545.

Host Integrity is a part of Symantec Network Access Control. The Host Integrity Policy ensures that computers meet your IT guidelines and corrects security problems that it finds. You can use Host Integrity alone, with a Quarantine Policy for self-enforcement, or with a network Enforcer Appliance. The Host Integrity Policy is most effective when used with an optional Enforcer, since the Appliance can ensure that every computer has a client and is properly configured before the client can connect to the network. The Enforcer can be either a hardware appliance that uses one of several types of Enforcer software or several Enforcers that are software-based only. When combined with the Enforcer, Host Integrity allows or

blocks computers from network access. Each Enforcer is designed for differing network needs.

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





# Setting up domains, groups, and clients

This chapter includes the following topics:

- [About your security topology](#)
- [About your group structure](#)
- [About importing the organizational structure](#)
- [Adding a domain](#)
- [Administering a domain](#)
- [Adding a group](#)
- [Deleting a group](#)
- [Renaming a group](#)
- [Moving a group](#)
- [Viewing a group's properties](#)
- [Adding clients as users](#)
- [Adding clients as computers](#)
- [Switching the client between user-based mode and computer-based mode](#)
- [Blocking clients from being added to groups](#)
- [Moving clients between groups](#)
- [Deleting clients](#)

- [Viewing a client's properties](#)
- [Searching for clients](#)
- [Filtering the list of clients](#)

## About your security topology

Your network's protection setup can be referred to as your security topology. Security topology refers to the security configuration of your enterprise, including the actual hardware and software components of servers and clients. You need to understand your network's security topology to protect your computers effectively from virus infections and other threats. Several tools help you understand your security topology. One tool is to create a map, or use a map that you currently have, to view the logical location of your client computers. Design this map so you can systematically isolate and clean the computers in each section before reconnecting them to your local network.

## About your group structure

The organizational structure for Symantec Endpoint Protection consists of domains, groups, users, and computers. The idea of groups is central to setting up your structure. It is very similar to the concept of user groups in Windows. The purpose of groups is to simplify your application of security policies. Instead of assigning them to each individual client computer, you can assign them to a group, or to multiple groups.

Groups are collections of client computers. The Symantec Endpoint Protection Manager server manages these client computers. These collections can be based on different parameters. For example, the group can be based on geography (all clients in a branch office). It can also be based on organization (all clients in the Sales department). Define your groups in a way that corresponds to your organizational structure. A user is a client defined by the logon name. A computer is a client defined by the physical piece of hardware.

You can create and organize groups in a hierarchical tree structure to represent the structure of your business. You assign security policies to groups and locations within those groups. Therefore, the creation of groups can be one of the first things administrators do when they configure Symantec Endpoint Protection Manager. You can then define the security policies which are based on the security needs of each group and apply them by using the Manager.

Groups, users, and computers can be added manually, imported from a directory server, or added automatically by client registration.

You can also import the organizational unit (OU) from a directory server (LDAP or Active Directory). Set up your organizational structure in this way. This structure automatically synchronizes the groups on Symantec Endpoint Protection Manager with those groups on the directory server.

See [“About importing the organizational structure”](#) on page 54.

## About domains

Domains are a way to contain groups, and groups contain computers and users, or clients. An administrator manages these computers and users. This administrator has a limited view of the Symantec Endpoint Protection Manager console.

You typically set up domains as part of a large enterprise. For example, a domain can represent a division within a company, department, separate company, or any other isolated segment of users. A small or a medium business model often would not be divided into domains.

System administrators have access to all domains while domain administrators can access only the domain they are assigned to work in. All data in each domain is completely separate. This separation prevents administrators in one domain from viewing data in other domains. In addition, administrators have no access to the Servers icon on the Admin page and you can further restrict their access within the console.

See [“About administrators”](#) on page 67.

## About groups

The purpose of groups and domains is to provide administrators with a way to manage sets of computers as one unit. All clients on an enterprise network are organized into groups with similar security needs and settings. Groups can contain the clients that are added as users or computers. You can create a group that is based on location, department, or any other classification that meets your business needs.

The group structure you define most likely matches the organizational structure of your company. You can group together users and computers with similar computing needs and network access requirements. You can manage these groups by using the Symantec Endpoint Protection Manager Clients tab. When you select a group in the View Clients tree, four page tabs are displayed in the page on the right. Each of these tabs is associated with managing the selected group. The four tabs are Clients, Policies, Details, and Install Packages. Each of these tabs provides different options for managing the selected group.

The Global group is the root of the hierarchical tree structure. Below it, you can add groups and subgroups to reflect your organization's structure. The hierarchical tree structure also includes the Temporary group by default. Users and computers are not always assigned to a group at the time they first register themselves with Symantec Endpoint Protection. They are assigned to the Temporary group when they do not belong to a predefined group.

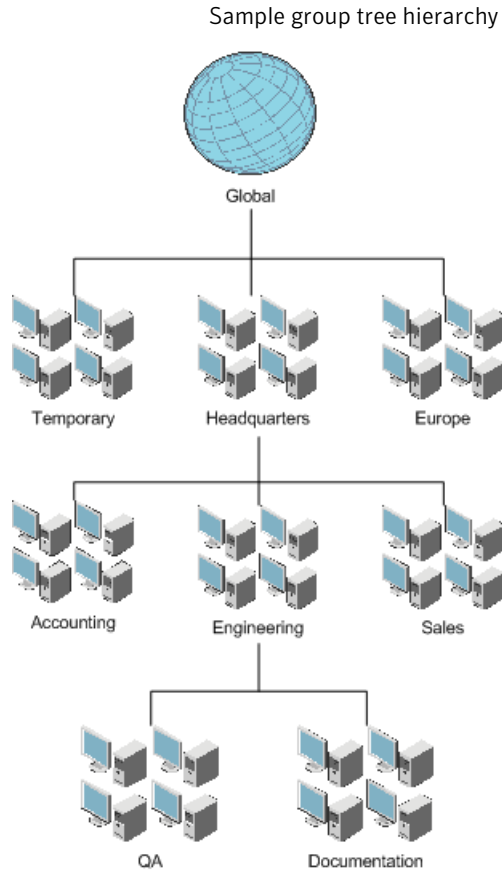
---

**Note:** You cannot create subgroups under the Temporary group.

---

[Figure 3-1](#) for an example of an organization's group tree hierarchy. Base your organization's group structure on the location, department, or any other classification that meets your business requirements.

**Figure 3-1**



If you create an install package for deployment, you can include security policies for a specific group. In this case, that group becomes the preferred client group. After the Symantec Endpoint Protection client software is installed it connects to the network. It is automatically added to the preferred client group unless some other Symantec Endpoint Protection Manager setting overrides it. For example, you may have manually added a user or a computer to a different group on the Clients tab. After the client connects to Symantec Endpoint Protection Manager, the group that is specified on the Clients page overrides the one that is specified in the install package. You can add the client in different groups either as a computer or as a user. The client connects to the group to which it was added in computer mode. The group that was specified in the client package may have previously been deleted. The client is placed in this default group when no other group has been specified for the user or for the computer on the Clients page.

If you import users from an Active Directory server, the group structure is also imported.

## About clients

A client is any network device that connects to the enterprise network and runs network-based applications. Network devices can include laptops, desktop computers, and servers.

A client software package is deployed to each computer or device within the network. Two types of clients exist: Symantec Endpoint Protection clients and Symantec Network Access Control clients. Symantec Endpoint Protection clients are installed on the computers that rely on Symantec Endpoint Protection for all of their firewall needs. Symantec Network Access Control clients are installed on the computers that do not require a firewall or that already have a third-party firewall.

You can run both types of clients your network. You can also change the type of client software on a computer if the firewall needs of the computer change. Use the Clients tab in the Symantec Endpoint Protection Manager to manage these settings.

You can apply different security policies to different locations. For example, the client can be set up to switch automatically to a different security policy if the physical location of the client changes. One policy might apply when the client connects at the office and another when the client connects remotely.

---

**Note:** Host Integrity check functionality is an add-on to the default product feature set.

---

## About user-based mode and computer-based mode

You can set up clients as users or computers, depending on how you want your security policies to work. Clients that are set up as users are based on the name of the user who logs on to the network. Clients that are set up as computers are based on the computer that logs on to the network. You set up clients as users or computers by adding the users and computers to an existing group. After a user or a computer is added to a group, it assumes the security policy that was assigned to the group.

A conflict can arise, such as when a user in one group logs on to a computer in another group. The security policy that is delivered depends on the mode in which the client software runs. The mode can be either computer-based or user-based. If the mode is user-based, the client computer software gets the policy from the group of which the user is a member. If the mode is computer-based, the client gets the security policy from the group of which the computer is a member.

Clients that are set up as users are considered to be in user-based mode. Clients that are set up as computers are considered to be in computer-based mode. Computer-based mode always takes precedence over user-based mode. Most administrators define clients as computers when there is a computer located in an unsecured area, like a lobby. That way, administrators can control the security policy no matter who logs on.

After you add a computer, it defaults to computer-based mode. That way, users who log on to the computer are restricted to the policy that is applied to the group to which the computer belongs. The policy that is applied to another group does not restrict these users. These users are not restricted even though they may be associated with other groups by user name.

You can add, delete, and move users and computers. You can also set computers to be unmanaged detectors on the network.

## About importing the organizational structure

You can import group structures, or organizational units. To import the organizational units, you use an LDAP directory server or an Active Directory server. Symantec Endpoint Protection can then automatically synchronize the groups on the Clients tab with those on the directory server.

See [“About organizational units and the LDAP server”](#) on page 241.

You cannot use the Clients tab to manage these groups after you import them. You cannot add, delete, or move groups within an imported organizational unit. You can assign security policies to the imported organizational unit. You can also copy users from an imported organizational unit to other groups that are listed

in the View Clients pane. The policy that was assigned to a group before it was imported has priority. A user account can exist in both the organizational unit and in an outside group. The policy that was applied to the outside group has priority in this scenario.

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

See [“Importing information about users from an LDAP directory server”](#) on page 237.

See [“Importing organizational units from an active or LDAP directory server”](#) on page 241.

See [“Adding directory servers”](#) on page 235.

See [“Synchronizing user accounts between directory servers and a Symantec Endpoint Protection Manager”](#) on page 237.

See [“Synchronizing organizational units”](#) on page 242.

## Adding a domain

Only a system administrator can see all the domains in an enterprise network. If you want a group to be in more than one domain, you add the group multiple times.

---

**Note:** You can add 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 in any client.

---

### To add a domain

- 1 In the console, click **Admin**.
- 2 On the Admin page, under Tasks, click **Add Domain**.
- 3 In the Add Domain dialog box, type a domain name and optional company name.
- 4 In the Contact List text box, optionally type the additional information, such as the name of the person who is responsible for that site.
- 5 If you want to add a domain ID, click **Advanced >>** and type the value in the Domain ID text box.
- 6 Click **OK**.

## Administering a domain

If you are a system administrator, you can create and administer domains. Domain administrators and limited administrators cannot create and administer domains.

### To administer a domain

- 1 In the console, click **Admin**.
- 2 On the Admin page, in the Tasks pane, click **Domains**.
- 3 Under View Domains, click the domain that you want to administer.  
You cannot administer a default domain.
- 4 Under Tasks, click **Administer Domain**.
- 5 Click **Yes** to confirm that you want to administer this domain.
- 6 In the dialog box that identifies the administered domain, click **OK**.

## Adding a group

You can add groups after you define the group structure for your organization. The group structure most likely matches the organizational structure of your company. Group names may be up to 256 characters long. Group descriptions may be up to 1024 characters long. Group names and descriptions may contain any character except the following characters: ["/\ \* ? < > | :].

---

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

---

### To add a group

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

## Deleting a group

You can delete the groups that you no longer use or that no longer reflect your organizational structure. You can delete a group only when it is empty. It cannot contain any subgroups, users, or computers. If a group is not empty, you must



first either move or delete the subgroups, users, or computers. In addition, you cannot delete the Global group or the Temporary group.

Under certain conditions, Symantec Endpoint Protection Manager recreates a deleted group for a client. This condition can include the following situation. An installation package (either an update package or a new installation package) is created specifying that group before the group is deleted. In addition, the installation setting Maintain existing client features when updating is enabled for that installation package. In this case, when the client computer connects to the management server, the server recreates the group that was specified in the installation package.

#### To delete a group

- 1 In the console, click **Clients**.
- 2 On the Clients tab, under View Clients, right-click the group that you want to delete, and click **Delete**.
- 3 In the Delete dialog box, click **Yes**.

## Renaming a group

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

#### To rename a group

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

## Moving a group

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

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

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

**To move a group**

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

## Viewing a group's properties

Each group has a property page. This page lists information about the group.

**To view a group's properties**

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

## Adding clients as users

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

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

**To add clients as users**

- 1 In the console, click **Clients**.
- 2 On the Clients page, under View Clients, locate the group to which you want to add a client.
- 3 On the Clients tab, under Tasks, click **Add User Account**.
- 4 In Add User for *group name* dialog box, in the User Name text box, type the name of the new user.
- 5 Under Domain Name, choose whether to log on to a specified domain or to log on to the local computer.
- 6 In the Description text box, type an optional description of the user.
- 7 Click **OK**.

## Adding clients as computers

Computers can be added to any group within Symantec Endpoint Protection Manager. The main reason to add a computer to a group is to protect that computer. That group's security policies protect the computer. For example, a computer may be located in a vulnerable place such as a public lobby. In this scenario, the computer gets added to a group of other public computers. The security policies that are applied to this group are applied to each computer within the group.

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

- You can add a computer to more than one group.
- You must know the actual computer name and the domain before you can add a computer.
- The maximum length of the computer name is 64 characters.
- The maximum length of the description field is 256 characters.

You can manually add a computer to a specific group and then install the client with a preferred group assigned to it. Do this task by associating group policies during package creation. In this case, the client is added to the group that is specified on the server. The client is not added to the group that is specified in the install package.

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

See [“Blocking clients from being added to groups”](#) on page 61.

### To add clients as computers

- 1 In the console, click **Clients**.
- 2 On the Clients page, under View Clients, locate the group to which you want to add a client.
- 3 On the Clients tab, under Tasks, click **Add Computer Account**.
- 4 In the Add Computer dialog box, type the name of the computer and the domain that you want the computer to be added to.
- 5 In the Description text box, optionally type a short description of the computer.
- 6 Click **OK**.

## Switching the client between user-based mode and computer-based mode

Clients can run in two different modes: computer-based mode or user-based mode. Computer-based mode always takes precedence over user-based mode. The client on the computer to which a user logs on uses the policy of the group to which the user belongs. This type of switch occurs when the computer is set to user-based mode.

If you switch from user-based mode to computer-based mode, consider the following situations:

- The computer name may not already be contained in any group. Switching to computer-based mode deletes the user name of the client from the group and adds the computer name of the client into the group.
- The computer name of the client and the user name are both in the same group. Switching from user-based mode to computer-based mode deletes the user name from the group and the client takes on the computer name.
- The computer name of the client is contained in a different group than the user name. Switching to computer-based mode changes the group of the client to the computer's group. A pop-up message informs you of the group's name change.

When the client is in computer-based mode, the client uses the policy of the group to which the computer belongs. The applied policy is independent of who logs on to the computer.

If you switch from computer-based mode to user-based mode, consider the following situations:

- The logon user name is not already contained in any group. Switching to user-based mode deletes the computer name of the client from the group. It then adds the user name of the client into the group.
- The group may contain both the logon user name of the client and the logon user name of the computer. Switching from computer-based mode to user-based mode deletes the computer name from the group. The client takes on the user name.
- The computer name of the client is contained in a different group from the user name. Switching to user-based mode changes the group of the client to the user's group. A pop-up message informs you of the group's name change.

#### To switch the client between user-based mode and computer-based mode

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

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

## Blocking clients from being added to groups

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

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

---

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

---

#### To block clients from being added to groups

- 1 In the console, click **Clients**.
- 2 Under **View Clients**, select the group for which you want to block new clients.

- 3 Click the **Details** tab.
- 4 On the Details tab, under Tasks, click **Edit Group Properties**.
- 5 In the Group Properties for *group name* dialog box, click **Block New Clients**.
- 6 Click **OK**.

## Moving clients between groups

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

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

### To move clients between groups

- 1 In the console, click **Clients**.
- 2 On the Clients page, under View Clients, locate the group that contains the clients that you want to move.
- 3 On the Clients tab, right-click the clients you want to move and click **Move**.  
Use the Shift key or the Control key to select all clients or specific clients.
- 4 In the Move Group: *group name* dialog box, select the group to which you want to move the selected clients.
- 5 Click **OK**.

## Deleting clients

You can delete users and computers from any group in Symantec Endpoint Protection Manager. Be careful when deleting users and computers. Deleting users and computers can affect the security policy that runs on the client.

By default, Symantec Endpoint Protection Manager automatically deletes inactive clients after 30 days. You can disable or change this option as a site property setting on the Servers tab.

See [“Editing site properties”](#) on page 226.

A client can be running when you manually delete it from a group. When the client next connects to Symantec Endpoint Protection Manager, it is registered again and the rules for client registration apply.

If your group structure includes both groups and imported organizational units, and a client is in computer-based mode, the following rules apply:

- The client switches to an organizational unit if the computer name exists there.
- The client registers itself again with the server.

If a client is in user-based mode, the following rules apply:

- The client switches to an organizational unit if the user name exists there.
- The client registers itself again with the server.

#### To delete clients

- 1 In the console, click **Clients**.
- 2 On the Clients page, under View Clients, locate the group that contains the clients that you want to remove.
- 3 On the Clients tab, select the clients you want to remove.  
Use the Shift key or the Control key to select all clients or specific clients.
- 4 Under Tasks, click **Delete Clients**.
- 5 In the Delete dialog box, click **Yes**.

## Viewing a client's properties

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

The page includes the following tabs:

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

See [“Collecting user information”](#) on page 79.

#### To view a client's properties

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

## Searching for clients

You may need to search for a specific client when you have many groups and clients in your domain. You can define the search criteria by the type of data that the management server collects about the client and that you request from the user.

---

**Note:** To successfully search on most of the information about the clients, you need to collect user information during the client software installation or later. This information is also displayed in the General tab and the User Info tab in the client's properties dialog box.

---

See [“Viewing a group's properties”](#) on page 58.

See [“Collecting user information”](#) on page 79.

#### To search for clients

- 1 In the console, click **Clients**.
- 2 On the Clients tab, under View Clients, choose the group you want to search.
- 3 Under Tasks, click **Search Clients**.
- 4 In the Search for Clients dialog box, in the Find drop-down list, select either Computers or Users.
- 5 Click **Browse** to search a different group.
- 6 In the Select Group dialog box, select the group and click **OK**.
- 7 Under Search Criteria, click the Search Field drop-down list and select the criteria by which you want to search.



- 8 Click the Comparison drop-down list and select a comparison operator.  
You can use standard Boolean operators in your search criteria.
- 9 In the Value cell, type the search string.
- 10 Click **Search**.
- 11 Click **Close** when you have finished searching for clients.

## Filtering the list of clients

You can use the filter feature to control which users and computers appear on the Clients tab.

You can also select how many clients appear on each page. When there are multiple pages, you can navigate through them by choosing either the Next icon or Previous icon. You can also skip directly to a particular page by typing the page number in the Page Number field.

### To filter the list of clients

- 1 In the console, click **Clients**.
- 2 In the View Clients pane, choose the group you want to search on.
- 3 In the Tasks pane, click **Set Display Filter**.
- 4 In the Set Display Filter dialog box, select one of the following options:
  - Show all Users and Computers
  - Show all Users
  - Show all Computers
  - Show Online Status (indicated by a green light next to the user name)
- 5 Set the number of clients that appear to a number that is between 1 and 5000.
- 6 Click **OK**.



# Managing administrators

This chapter includes the following topics:

- [About administrators](#)
- [About managing administrators](#)
- [Adding an administrator](#)
- [Switching between a non-limited and a limited administrator and configuring access rights](#)
- [Locking an administrator's account after too many logon attempts](#)
- [Authenticating administrators](#)
- [Renaming an administrator](#)
- [Changing an administrator's password](#)
- [Removing an administrator](#)

## About administrators

Symantec Endpoint Protection Manager uses administrators to implement its functionality. Three types of administrator roles are used: system administrator, administrator, and limited administrator. Each of these administrator roles has a different set of privileges and tasks to perform.

The system administrator is the super administrator of a system. An administrator who is designated as a system administrator can do anything in a system. An administrator is one level lower than a system administrator. An administrator is the super administrator within the domain that administrator manages. An administrator can neither create nor delete domains. An administrator also cannot access management servers or Enforcer servers. Limited administrators perform

the work that is assigned to them by the system administrator or administrator. In addition, they can configure their own attributes including security settings and notification settings.

[Table 4-1](#) lists the responsibilities for each administrator role.

**Table 4-1** Administrator types roles and responsibilities

Administrator role	Responsibilities
System administrator	<ul style="list-style-type: none"> <li>■ Manages domains.</li> <li>■ Creates and manages system administrators, administrators, and limited administrators.</li> <li>■ Manages servers.</li> </ul>
Administrator	<ul style="list-style-type: none"> <li>■ Manages a single domain</li> <li>■ Creates administrators and limited administrators within the domain.</li> <li>■ Deletes and modifies the administrators who are created within a single domain.</li> <li>■ Changes the attributes for the administrators who are created in the domain. These attributes include notifications, security, and permission settings.</li> </ul>
Limited administrator	<ul style="list-style-type: none"> <li>■ Manages access rights, reporting rights, and notification settings for specific groups within a single domain.</li> <li>■ Performs the work that the system administrator or administrator assigns.</li> <li>■ Cannot create, delete, or modify domains or other administrators.</li> <li>■ Cannot change the limited administrator's own access rights.</li> <li>■ Cannot configure the management server or Enforcer server.</li> </ul>

## About managing administrators

You can create the three types of administrators that are used: system administrators, administrators, and limited administrators. The administrators and the limited administrators are both domain administrators.

System administrators can view and modify the entire system, while administrators can view and modify only their own domains. System administrators have full access rights to all Symantec Endpoint Protection Manager pages and tabs.

Administrators have only reporting privileges. They have no access to the domains or servers, and you can restrict their access to other options.

The tasks an administrator can perform depend on the administrator type. For example:

- A system administrator sees all other system administrators, all administrators, and all limited administrators that are associated with the current domain.
- An administrator sees the domain and limited administrators that are associated with the domain the administrator currently administers.
- A limited administrator sees only itself.

When you install the Symantec Endpoint Security Manager, a default system administrator that is called `admin` is created.

You can view every other administrator who manages the domain into which the administrator is logged. This list includes all system administrators, administrators, and limited administrators.

## Adding an administrator

As your network expands or otherwise changes, you may find the number of administrators insufficient to meet your needs. At such point, you can add one or more administrators. As you add an administrator, you specify the administrator's capabilities and constraints. As a system administrator, you can add another system administrator, administrator, or limited administrator.

See [Table 4-1](#) on page 68.

The following list contains additional information about creating system administrators:

- System administrators have full access rights. You can also add administrators and limited administrators, both of which have more limited access rights.
- If you do not specify any access rights for an administrator, the administrator is created in a disabled state unable to log on.

See [“About administrators”](#) on page 67.

### To add an administrator

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

- 3 In the Add Administrator dialog box, enter the administrator name.  
This name is the name with which the administrator logs on and by which the administrator is known within the application.
- 4 Optionally enter the full name of the administrator in the second text box.  
This field is for informational purposes only.
- 5 Type and retype the password.  
The password must be six or more characters; all characters are permitted.
- 6 Specify the authentication type.  
The default value is Symantec Management Server Authentication. If you want to use the default value, skip to step 9.
- 7 If you want to change to another authentication type, click **Change**.
- 8 In the Administrator Authentication dialog box, choose one of the following options:
  - Symantec Management Server Authentication  
See [“Adding directory servers”](#) on page 235.
  - RSA SecurID Authentication  
See [“Configuring the Symantec Endpoint Protection Manager to use RSA SecurID Authentication”](#) on page 250.
  - Directory Authentication  
Then type the directory server and the account name into the appropriate text boxes.
- 9 Select one of the following administrator types:
  - System Administrator, and then skip to step 12.
  - Administrator, and then skip to step 10.
  - Limited Administrator, and then skip to step 11.
- 10 If you selected Administrator, click **Reporting Rights** to specify which reports the administrator can run, based on computers, IP addresses, server groups, client groups, and parent servers.  
Skip to step 12.
- 11 If you selected Limited Administrator, you can specify access rights by doing one or more of the following actions:
  - Check **View reports**, and then click **Reporting Rights**.
  - Check **Manage clients**, and then click **Group Rights**.

**Switching between a non-limited and a limited administrator and configuring access rights**

You can specify which groups the administrator has full access, read-only access, or no access to.

- Click **Manage policies**.

You can authorize the administrator to create only non-shared policies for a location by clicking **Only allow location-specific policy editing**.

12 Click **OK**.

## Switching between a non-limited and a limited administrator and configuring access rights

You can change a non-limited administrator to a limited administrator and you can change a limited administrator to a non-limited administrator. You can also change the access rights and reporting constraints for administrators and limited administrators.

### To switch between a non-limited and limited administrator and configure access rights

- 1 On the Symantec Endpoint Protection Manager console, click **Admin**.
- 2 On the Admin page, click **Administrators**.
- 3 Under View Administrators, select the administrator.
- 4 Under Tasks, click **Edit Administrator Properties**, and then click **Access Rights**.
- 5 On the Access Rights tab, do one of the following tasks:
  - Select Administrator, and then skip to step 7.  
If you migrated from Symantec AntiVirus 10.x and earlier, and you want the administrator to run reports for these migrated server groups, click **Reporting Rights**.
  - Select Limited Administrator.
- 6 Do one of the following actions:
  - Check **View reports**, and then click **Reporting Rights**.
  - Check **Manage clients**, and then click **Group Rights**.  
You can specify what level of access the administrator has to which groups.
  - Check **Manage policies**.  
To restrict the administrator to creating only non-shared policies for a location, click **Only allow location-specific policy editing**.
- 7 Click **OK**.

## Locking an administrator's account after too many logon attempts

You can lock the administrator's account if you think a user tries to log on to the management server too many times. You can also configure the management server to send an email message to the administrator to notify them after the administrator is locked out. This ability is useful if the person logging in is not the administrator.

You can configure the following settings for locking an administrator's account:

- The Failed Login Attempt value is reset to 0 after the administrator successfully logs on and later logs off.
- The administrator has the full number of attempts to log on again at a later time. After the administrator reaches the limit for unsuccessful logon attempts, the account is locked. The administrator must then wait for the specified number of minutes to wait before logging on again.

### To lock an administrator's account after too many logon attempts

- 1 On the Symantec Endpoint Protection Manager console, click **Admin**.
- 2 On the Admin page, click **Administrators**.
- 3 Under View Administrators, select the administrator.
- 4 Under Tasks, click **Edit Administrator Properties**.
- 5 On the General tab, in the Email text box, type the administrator's email address.

The management server sends an email message to this email address when the management server locks the administrator's account. You must check the **Send email alert when account is locked** check box to send the email message.

- 6 Under Log On Attempt Threshold, move the slider to set the number of permitted incorrect logon attempts.
- 7 To lock the account when the administrator has exceeded the number of logon attempts, click **Lock this account when log on attempts exceed the threshold**.
- 8 To send an email message to the administrator after the management server locks the administrator's account, check **Send an email alert when the account is locked**, and then set the number of minutes.
- 9 Click **OK**.



# Authenticating administrators

When you add an administrator, you can specify which authentication software the management server uses to authenticate administrator accounts.

You can authenticate administrators by using the management server with RSA SecurID. You must verify that you have an existing RSA Server and have already installed and configured the RSA SecurID server on a separate computer. Also verify that the RSA SecurID server can communicate with the SecurID Agent.

You can enable RSA security for administrator accounts on Symantec Endpoint Protection Manager.

The following RSA log on mechanisms are supported:

- RSA SecurID token (not software RSA tokens)
- RSA SecurID card
- RSA keypad card (not RSA smart cards)

## To authenticate administrators

- 1 On the Symantec Endpoint Protection Manager console, click **Admin**.
- 2 On the Admin page, click **Administrators**.
- 3 Under View Administrators, select the administrator.
- 4 Under Tasks, click **Edit Administrator Properties**, and then click **Authentication**.
- 5 On the Authentication tab, select one of the following authentication options that you want to use to authenticate the administrator's account:
  - Symantec Management Server Authentication  
See [“Adding directory servers”](#) on page 235.
  - RSA SecurID Authentication  
See [“Configuring the Symantec Endpoint Protection Manager to use RSA SecurID Authentication”](#) on page 250.
  - Directory Authentication  
Then type the directory server and the administrator's account name.
- 6 Click **OK**.

# Renaming an administrator

To change organizational responsibilities or assignments, you may want to change the name you have given to an administrator.

#### To rename an administrator

- 1 On the Symantec Endpoint Protection Manager console, click **Admin**.
- 2 On the Admin page, click **Administrators**.
- 3 Under View Administrators, select the administrator to rename.
- 4 Under Tasks, click **Rename Administrator**.
- 5 In the Rename Administrator for *name* dialog box, change the name, and then click **OK**.

## Changing an administrator's password

For security purposes, you may need to change an administrator's password.

When you first configured the management server in the Management Server Configuration Wizard, you could select a simple or an advanced installation. If you selected the simple installation, the password you entered is the same as the encryption password. If you change the administrator's password, the encryption password does not change.

#### To change an administrator's password

- 1 On the Symantec Endpoint Protection Manager console, click **Admin**.
- 2 On the Admin page, click **Administrators**.
- 3 Under View Administrators, select the administrator.
- 4 Under Tasks, click **Change Administrator Password**.
- 5 Enter and confirm the new password.

The password must be six or more characters in length, and all characters are permitted.

- 6 Click **OK**.

## Removing an administrator

You can remove an administrator when that administrator is no longer needed.

#### To remove an administrator

- 1 On the Symantec Endpoint Protection Manager console, click **Admin**.
- 2 On the Admin page, click **Administrators**.
- 3 Under View Administrators, select the administrator to remove.

- 4 Under the Tasks pane, click **Delete Administrator**.
- 5 In the Delete Administrator for *name* dialog box, click **Yes** to verify that you want to remove this administrator.



# Working with client installation packages

This chapter includes the following topics:

- [About client installation packages](#)
- [Configuring client installation package options](#)
- [Exporting client installation packages](#)
- [Adding client installation package updates and upgrading clients](#)
- [Deleting upgrade packages](#)

## About client installation packages

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

You can use the Symantec Endpoint Protection Manager Console to export these packages as a single executable file or as a series of files in a directory. The method that you choose depends on your deployment method and whether you want to upgrade client software in groups from the management console. The single executable is available for third-party installation tools and for potential bandwidth conservation. Typically, if you use Active Directory Group Policy Object, you would not choose to export to a single executable file.

During the export process, you select either the 32-bit installation packages or the 64-bit installation packages that are provided by default. You then optionally select the specific client protection technologies to install if you do not want to

install all components. You can also specify how the installation interacts with end users. Finally, you can install the exported files (a package) to computers one at a time, or deploy the exported files to multiple computers simultaneously.

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

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

## Configuring client installation package options

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

### Configuring installation package features

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

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

#### To configure installation package features

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

## Configuring client installation package settings

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

### To configure client installation package settings

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

## Collecting user information

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

---

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

---

### To collect user information

- 1 In the console, click **Admin**, and then click **Install Packages**.
- 2 Under View Install Packages, click **Client Install Packages**.
- 3 In the Client Install Packages pane, click the package for which you want to collect user information.
- 4 Under Tasks, click **Set User Information Collection**.
- 5 In the Set User Information Collection dialog box, check **Collect User Information**.

- 6 In the Pop-up Message text box, type the message that you want users to read when they are prompted for information.
- 7 If you want the user to have the ability to postpone user information collection, check **Enable Remind Me Later**, and then set a time in minutes.
- 8 Under Select the fields that appear for the user to provide input, choose the type of information to collect, and then click **Add**.  
  
You can select one or more fields simultaneously by pressing the Shift key or the Control key.
- 9 In the Optional column, check the check box next to any fields that you want to define as optional for the user to complete.
- 10 Click **OK**.

## Exporting client installation packages

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

For example, if you create an installation package for a group named MyGroup beneath Global, a directory named Global\_MyGroup gets created. This directory contains the exported installation package.

---

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

---

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



---

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

---

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

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

#### To export client installation packages

- 1 In the console, click **Admin**, and then click **Install Packages**.
- 2 Under View Install Packages, click **Client Install Packages**.
- 3 In the Client Install Packages pane, under Package Name, click the package to export.
- 4 In the lower-left pane, under Tasks, click **Export Client Install Package**.
- 5 In the Export Package dialog box, click **Browse**.
- 6 In the Select Export Folder dialog box, browse to and select the directory to contain the exported package, and then click **OK**.  
  
Directories with double-byte or high-ASCII characters are not supported and are blocked.
- 7 In the Export Package dialog box, set the other options according to your installation goals.
- 8 For details about setting other options in this dialog box, click **Help**.
- 9 Click **OK**.

## Adding client installation package updates and upgrading clients

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

with LiveUpdate if you permit clients to run LiveUpdate and if the LiveUpdate Settings Policy permits updates.

## Adding client installation package updates

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

---

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

---

### To add a client installation package update

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

- 12 For details about setting other options in this dialog box, click **Help**.
- 13 Click **OK**.

## Upgrading clients in one or more groups

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

---

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

---

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

- 1 If you have not already done so, display the Client Install Packages pane by completing the following steps:
  - In the console, click **Admin**.
  - Under Tasks, click **Install Packages**, and then click **Upgrade Groups with Package**.
- 2 In the Upgrade Groups Wizard panel, click **Next**.
- 3 In the Select Client Install Package panel, under Select the new client installation package, select the package that you added, and then click **Next**.
- 4 In the Specify Groups panel, check the groups that you want to upgrade, and then click **Next**.
- 5 In the Package Upgrade Settings panel, check **Download from the management server**, and then click **Next**.
- 6 In the Upgrade Groups Wizard Complete panel, click **Finish**.

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

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

For details about setting other options, click **Help**.

- 5 When you finish configuring the update distribution options, click **OK**.

## Deleting upgrade packages

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

---

**Note:** Do not delete the packages that are installed on your client computers.

---

### To delete upgrade packages

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

# Updating definitions and content

This chapter includes the following topics:

- [About LiveUpdate and updating definitions and content](#)
- [Configuring a site to download updates](#)
- [Configuring LiveUpdate Policies](#)
- [Advanced update distribution options](#)

## About LiveUpdate and updating definitions and content

LiveUpdate is the name of the technology that checks for and distributes definitions and content updates to client computers. These updates include virus and spyware definitions, IPS signatures, product updates, and so forth for Symantec Endpoint Protection clients. You can let end users run LiveUpdate on client computers, and you can schedule LiveUpdate to run on client computers at specified times. When LiveUpdate runs and determines that updates are required, LiveUpdate downloads and installs the updates that it is configured for and permitted to run.

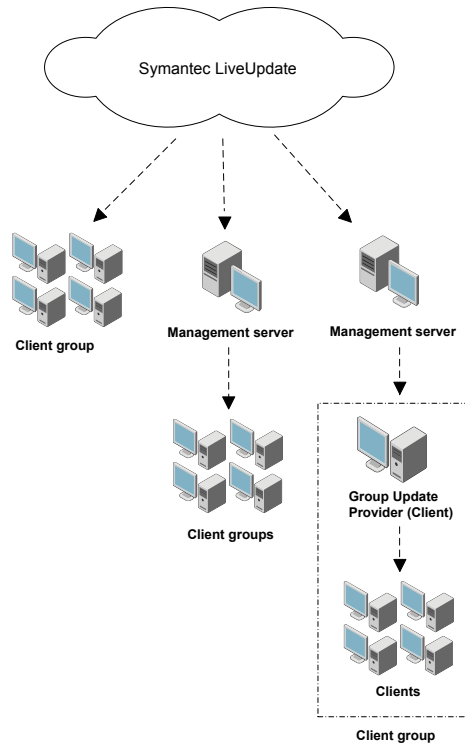
For Symantec Endpoint Protection, two different policies control how and when these updates are distributed to clients, and control the update types. With the first policy, you define the update server that client computers use, and define how often the clients check the server for updates. With the second policy, you define the type of updates for which you want clients to download from the server. For Symantec Network Access Control, only the first policy type is supported.

## About update network distribution architectures

Several network architectures are available to update clients. How you architect your network depends on bandwidth availability and conservation. Very small networks can schedule clients to get updates directly from Symantec. Small to medium networks of up to a couple thousand clients can use the default. The default is to have the Symantec Endpoint Protection Manager get updates from a Symantec LiveUpdate server, and then provide those updates to managed clients. Larger networks can introduce Group Update Providers.

Figure 6-1 illustrates these relatively simple architecture options.

Figure 6-1 Simple update distribution architecture options



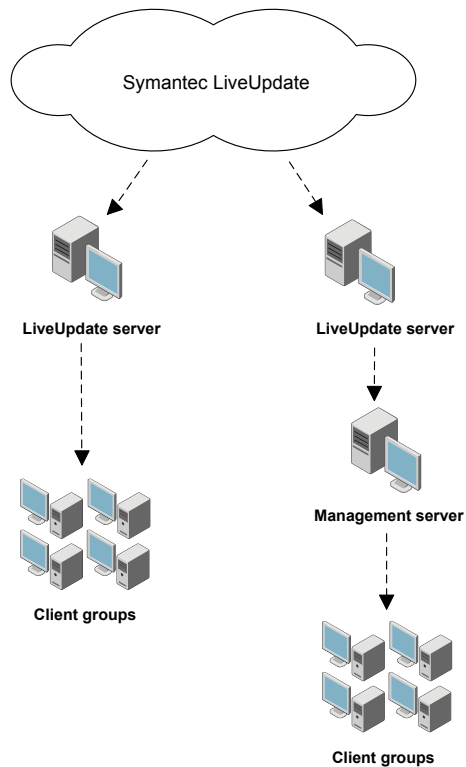
The Group Update Provider is an option that you can use in any group. When you create the LiveUpdate Policy for the group, you can specify one client to download updates. You can send the updates to the other clients in the group. The Group Update Provider does not have to be in the group, and can update multiple groups.

In large networks of more than 10,000 clients, an internal LiveUpdate server is available to conserve bandwidth. This architecture preserves processing power

at the management server. In this instance, you can configure the internal LiveUpdate server to download updates from a Symantec LiveUpdate server, and then send updates to client computers. With this architecture, the management server offloads the update functionality, but still processes logs and policy updates. The internal LiveUpdate server is also useful for the networks that run multiple Symantec products that also run LiveUpdate to update clients.

Figure 6-1 illustrates these more complex architecture options.

**Figure 6-2** More complex update distribution architecture options




---

**Note:** Two additional architecture options are available. One option provides for third-party management with tools like Microsoft SMS and IBM Tivoli. The other option provides for a proxy server that sits between the internal LiveUpdate server and the management servers and clients that it updates. For details on the proxy server, refer to the *LiveUpdate Administrator's Guide* on the installation CD.

---

Table 6-1 describes the most common architecture options.

**Table 6-1** Update distribution architecture options

Architecture	Description	When to use it
Symantec Endpoint Protection Manager to clients (Default)	By default, Symantec Endpoint Protection Managers update the clients that they manage, and the management servers pull these updates from the site database. The site database typically received updates from a Symantec LiveUpdate server.	Initially use this architecture as it is the easiest method to implement and is installed and configured by default after management server installation. You can also combine this method with a Group Update Provider.
Group Update Provider to clients	A Group Update Provider is a client that acts as a proxy between a Symantec Endpoint Protection Manager and the clients in the group. The Group Update Provider receives updates from a management or LiveUpdate server, and then forwards the updates to the other clients in the group. A Group Update Provider can update multiple groups.	Use this method for groups co-located at remote locations with minimal bandwidth. Also, this method reduces the load on the management servers.
LiveUpdate server to clients	Clients can pull updates directly from a LiveUpdate server. The LiveUpdate server can be an external Symantec LiveUpdate server, or an internal LiveUpdate server that receives updates from an external Symantec LiveUpdate server.	Use the external Symantec LiveUpdate server for the unmanaged client computers that are not always connected to the corporate network. Use the internal LiveUpdate server in large networks to reduce the load on the Symantec Endpoint Protection Manager server.  <b>Note:</b> Do not configure large numbers of managed, networked clients to pull updates from an external Symantec LiveUpdate server. This configuration consumes unnecessary amounts of Internet gateway bandwidth.
Third-party tool distribution (Not illustrated)	Third-party tools like Microsoft SMS let you distribute specific update files to clients. You can retrieve Intelligent Updater self-extracting files from the Symantec Web site that contain virus and security risk definitions files with jdb and vdb extensions. Idb extensions are no longer supported. To receive other update files, you must set up and configure a Symantec Endpoint Protection Manager server to download and stage the update files.	Use this method when you want to test update files before distributing them. Also, use this method if you have a third-party tool distribution infrastructure, and want to leverage the infrastructure.



## About update types

By default, client computers receive all of the latest update types unless a policy is applied that restricts or prohibits the update types. If a group uses the Symantec Endpoint Protection Manager to distribute updates (the default), then the management server must also be configured to download the same updates. Otherwise, those updates are not available for group distribution.

[Table 6-2](#) lists and describes the update types.

**Table 6-2** Update types

Update type	Description
Antivirus and antispyware definitions	These definitions contain two types of updates, full-version update and direct-delta update. The type of the update is included in the update package. Separate virus definition packages are available for the x86 and the x64 platforms.
Decompiler signatures	These signatures support the Antivirus and Antispyware protection engine, and are used to decompose and read the data that is stored in various formats.
TruScan proactive threat scan heuristic signatures	These signatures protect against zero-day attack threats.
TruScan proactive threat scan commercial application list	These application lists are legitimate commercial applications that have generated false positives in the past.
Intrusion Prevention signatures	These signatures protect against network threats and support the intrusion prevention and detection engines.
Submission Control signatures	These signatures control the flow of submissions to Symantec Security Response.

## Configuring a site to download updates

Configuring and scheduling update downloads is a two-part process. First, you configure a site to download updates. The site must contain the updates that are distributed to clients. The updates are distributed to clients as specified in the LiveUpdate Policies that are applied to the locations in a group.

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

- How often to check for updates.
- What update types to download.

LiveUpdate Policies also specify what updates types to download to clients. Be sure that the site downloads all updates that are specified in client LiveUpdate Policies.

- The languages for update types to download.
- The LiveUpdate server that serves the updates to the site.  
You can specify either an external Symantec LiveUpdate server (recommended), or an internal LiveUpdate server that has previously been installed and configured.
- The number of content revisions to keep and whether to store the client packages unzipped.

You can set up an internal LiveUpdate server on a computer whether Symantec Endpoint Protection Manager software is installed or not. In either case, you should use the LiveUpdate Administrator utility to update the LiveUpdate server. The LiveUpdate Administrator utility pulls the definitions updates down from a Symantec LiveUpdate server. The utility then places the packages on a Web server, an FTP site, or a location that is designated with a UNC path. You must then configure your Symantec Endpoint Protection Managers to pull their definitions updates from this location.

For more information, see the *LiveUpdate Administrator's Guide*, which is available on the installation CD and on the Symantec Support Web site.

If replication is used, only one site needs to be configured to download update files. Replication automatically updates the other database. As a best practice, however, you should not replicate product updates between sites. These updates can be quite large and one exists for every language that you select. If you select to download product updates with LiveUpdate to Symantec Endpoint Security Manager, the updates automatically appear in the Installation Packages pane. You can then update clients with auto-upgrade. If you use this approach for version control, you should not select automatic product upgrades in the LiveUpdate Settings Policy.

---

**Note:** Sites download MSP files for product updates, and then create new MSI files. Sites replicate MSI files if you select to replicate product updates. The MSP files are a fraction of the size of the MSI files. The default schedule of having Symantec Endpoint Protection Manager run LiveUpdate every 4 hours is a best practice.

---

#### To configure a site to download updates

- 1 On the console, click **Admin**.
- 2 In the Tasks pane, click **Servers**.

- 3 In the View pane, right-click **Local Site**, and then click **Properties**.
- 4 In the Site Properties dialog box, on the LiveUpdate tab, under Download Schedule, set the scheduling options for how often the server should check for updates.
- 5 Under Content Types to Download, inspect the list of update types that are downloaded.
- 6 To add or delete an update type, click **Change Selection**, modify the list, and then click **OK**.
- 7 Under Languages to Download, inspect the list of languages of the update types that are downloaded.
- 8 To add or delete a language, click **Change Selection**, modify the list, and then click **OK**.
- 9 Under LiveUpdate Source Servers, inspect the current LiveUpdate server that is used to update the management server. This server is Symantec LiveUpdate server by default. Then do one of the following:
  - To use the existing LiveUpdate Source server, click **OK**. Do not continue with this procedure; you are finished.
  - To use an internal LiveUpdate server, click **Edit Source Servers**, and continue with this procedure.
- 10 In the LiveUpdate Servers dialog box, check **Use a specified internal LiveUpdate server**, and then click **Add**.
- 11 In the Add Update Server dialog box, complete the boxes with the information that identifies the LiveUpdate server, and then click **OK**.
- 12 In the Site Properties dialog box, under Disk Space Management for Downloads, type the number of LiveUpdate content revisions to keep and decide whether to choose the Store client packages unzipped check box.
 

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

Help lists and describes the data to enter in the boxes. For failover support, you can install, configure, and select more than one LiveUpdate server. If one server goes offline, the other server provides support.

## Configuring LiveUpdate Policies

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

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

### Configuring a LiveUpdate Settings Policy

When you add and apply a LiveUpdate Settings Policy, you should have a plan for how often you want client computers to check for updates. The default setting is every 4 hours. You should also know from where you want your client computers to check for and get updates. Generally, you want client computers to check for and get updates from the Symantec Endpoint Protection Manager. After you create your policy, you can assign the policy to one or more groups and locations.

---

**Note:** An advanced setting is available to let users manually start LiveUpdate from their client computers and the setting is disabled by default. If you enable this setting, users can start LiveUpdate and download the latest content virus definitions, component updates, and potential product updates. If the advanced policy setting for Download product updates using LiveUpdate is enabled, the product updates that they download are maintenance releases and patches for Symantec client software. Depending on the size of your user population, you may not want to let users download all content without previous testing. Additionally, conflicts can occur if two LiveUpdate sessions run simultaneously on client computers. A best practice is to leave this setting disabled.

---

#### To configure a LiveUpdate Settings Policy

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

- 4 In the Overview pane, in the Policy name box, type a name for the policy.
- 5 Under LiveUpdate Policy, click **Server settings**.
- 6 In the Server Settings pane, under Internal or External LiveUpdate Server, check and enable at least one source from which to retrieve updates.  
Most organizations should use the default management server.
- 7 If you selected Use a LiveUpdate server, under LiveUpdate Policy, click **Schedule**.
- 8 In the Schedule pane, accept or change the scheduling options.
- 9 If you selected Use a LiveUpdate server, under LiveUpdate Policy, click **Advanced Settings**.
- 10 Decide whether to keep or change the default settings.

Generally, you do not want users to modify update settings. You may, however, want to let them manually launch a LiveUpdate session if you do not support hundreds or thousands of clients.

- 11 When you have configured your policy, click **OK**.
- 12 In the Assign Policy dialog box, do one of the following:
  - Click **Yes** to save and assign the policy to a group or location in a group.
  - Click **No** to save the policy only.
- 13 If you clicked Yes, in the Assign LiveUpdate Policy dialog box, check the groups and locations to which to assign the policy, and then click **Assign**.  
If you cannot select a nested group, that group inherits policies from its parent group, as set on the Computers and Users Policies tab.

## Configuring a LiveUpdate Content Policy

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

See [“Configuring a site to download updates”](#) on page 89.

If a group is configured to get updates from a LiveUpdate server, the group's clients receive all updates permitted in the LiveUpdate Content Policy. If the LiveUpdate Content Policy specifies a specific revision for an update, the clients never receive updates for this particular update until the setting is changed from

a specific revision to the latest available. LiveUpdate servers do not understand named version functionality.

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

---

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

---

### To configure a LiveUpdate Content Policy

- 1 On the console, click **Policies**.
- 2 In the View Policies pane, click **LiveUpdate**.
- 3 On the LiveUpdate Content tab, click **Add a LiveUpdate Content Policy**.
- 4 In the Overview pane, in the Policy name box, type a name for the policy.
- 5 In the LiveUpdate Content pane, click **Security Definitions**.
- 6 In the Security definitions pane, check the updates to download and install, and uncheck the updates to disallow.
- 7 For each update, do one of the following actions:
  - Check **Use latest available**
  - Check **Select a revision**
- 8 To continue, do one of the following:
  - If you did not check Select a revision for an update type, click **OK**, and then continue with step [11](#).
  - If you did check Select a revision for an update type, click **Edit**, and then continue with the next step.
- 9 In the Select Revision dialog box, in the Revision column, click and select the revision to use, and then click **OK**.
- 10 In the LiveUpdate Content window, click **OK**.
- 11 In the Assign Policy dialog box, click **Yes**.

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

## Viewing and changing the LiveUpdate Content Policy that is applied to a group

LiveUpdate Content Policies are applied to groups and to all locations in groups. Therefore, the policy does not appear with other policies under locations in the console.

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

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

## Configuring a Group Update Provider in a LiveUpdate Settings Policy

When you create a LiveUpdate Settings Policy, you have the option of specifying a Group Update Provider. The Group Update Provider provides updates to clients in the group, and any subgroups that inherit policies as set on the Clients tab. If you have clients in a group at a remote location that have bandwidth issues over the WAN, make a client in the group the Group Update Provider, and then configure the group to use that Group Update Provider. The Group Update Provider also lets you offload processing power from the Symantec Endpoint Protection Manager if you need that option.

---

**Note:** You can configure a Group Update Provider when you create a policy, or you can configure one when you modify an existing policy. You should first create a policy without a Group Update Provider and verify that client computers receive updates. Upon verification, you can then add a Group Update Provider. This approach helps troubleshooting communication problems. However, if the Group Update Provider computer goes offline, the clients in the group get updates directly from its management server.

---

When you configure a Group Update Provider, you specify a host name or IP address and a TCP port number. The default TCP port number is 2967, a port that was used in Symantec AntiVirus 10.x and Symantec Client Security 3.x network

communications. If your Group Update Provider computer receives IP addresses with DHCP, you should either assign a static IP address to the computer, or type the host name. If your Group Update Provider computer is at a remote location, and if that remote location uses network address translation (NAT), type the host name.

---

**Note:** If the Group Update Provider runs a Windows firewalls or the Symantec Client Firewall, you must modify the Firewall Policy to permit TCP port 2967 to receive communications from the Symantec Endpoint Protection Manager.

---

#### To configure a Group Update Provider in a LiveUpdate Settings Policy

- 1 On the console, click **Policies**.
- 2 In the View Policies pane, click **LiveUpdate**.
- 3 In the LiveUpdate Policies pane, on the LiveUpdate Settings tab, under Name, select the policy to edit.
- 4 In the Tasks pane, click **Edit the Policy**.
- 5 In the LiveUpdate Policy window, click **Server Settings**.
- 6 On the LiveUpdate Server tab, under Local Network server Option, check **Use the Group Update Provider as the default LiveUpdate server**.
- 7 Click **Group Update Provider**.
- 8 In the Group Update Provider dialog box, in the Host box, type an IP address or a host name.
- 9 In the Port box, accept or change the default, and then click **OK**.

## Advanced update distribution options

You can use Intelligent Updater to distribute virus and security risk updates. You can also use third party distribution tools to distribute updates. You get these updates after you install and configure a Symantec Endpoint Protection Manager to download the updates that you want to distribute.

---

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

[ftp://ftp.symantec.com/AVDEFS/symantec\\_antivirus\\_corp/](ftp://ftp.symantec.com/AVDEFS/symantec_antivirus_corp/)

---



## Providing antivirus content updates with Intelligent Updater

To distribute updated virus and security risk updates only, download a new Intelligent Updater. Then, use your preferred distribution method to deliver the updates to your managed servers and clients. Intelligent Updater is available as a single file or as a split package, which is distributed across several smaller files. The single file is for computers with network connections. The split package is for the computers that do not have network connections, Internet access, or a CD-ROM drive. Copy the split package to removable media for distribution.

---

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

---

### To download Intelligent Updater

- 1 Using your Web browser, go to the following URL:  
<http://securityresponse.symantec.com>
- 2 Under **Virus Definitions**, click **Download Virus Definitions Manually**.
- 3 Click **Download Virus Definitions (Intelligent Updater Only)**.
- 4 Select the appropriate language and product.
- 5 Click **Download Updates**.
- 6 Click the file with the .exe extension.
- 7 When you are prompted for a location in which to save the files, select a folder on your hard drive.

### To install the virus and security risk definitions files

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

## About using third party distribution tools to distribute updates to managed clients

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

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

See “[Configuring a site to download updates](#)” on page 89.

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

```
\\Program Files\Symantec Endpoint Protection Manager\data\outbox\
```

You then distribute the files to the inbox directories on client computers:

The following directory appears on the client computers that do not run Windows Vista:

```
\\Documents and Settings\All Users\Application Data\Symantec\Symantec Endpoint Protection\inbox\
```

The following directory appears on the client computers that do run Windows Vista:

```
\\Program Data\Symantec\Symantec Endpoint Protection\inbox\
```

By default, this directory does not exist, and client software does not check and process content in this directory. For managed clients, you must configure a LiveUpdate Policy for the group, enable third party distribution to clients in the group, and apply the policy. For unmanaged clients, you must manually enable a registry key.

---

**Note:** A best practice is to enable this support with a LiveUpdate Policy.

---

## Enabling third party content distribution to managed clients with a LiveUpdate Policy

When you create a LiveUpdate Policy that supports third party content distribution to managed clients, you have a couple of additional goals. One goal is to reduce the frequency with which clients check for updates. The other goal typically is to disable the ability of client users to manually perform LiveUpdate. The term managed clients means that the clients are managed with Symantec Endpoint Protection Manager policies.

When you are finished with this procedure, the following directory appears on the group's client computers that do not run Windows Vista:

```
\\Documents and Settings\All Users\Application Data\Symantec\Symantec Endpoint Protection\inbox\
```

The following directory appears on the group's client computers that do run Windows Vista:

```
\\Program Data\Symantec\Symantec Endpoint Protection\inbox\
```

### To enable third party content distribution to managed clients with a LiveUpdate Policy

- 1 On the console, click **Policies**.
- 2 In the View Policies pane, click **LiveUpdate**.
- 3 In the LiveUpdate Policies pane, on the LiveUpdate Settings tab, under Tasks, click **Add a LiveUpdate Setting Policy**.
- 4 In the LiveUpdate Policy window, in the Policy name and Description boxes, type a name and description.
- 5 Under Third Party Management, check **Enable third party content management**.
- 6 Uncheck all other LiveUpdate source options.
- 7 Click **OK**.
- 8 In the Assign Policy dialog box, click **Yes**.  
You can optionally cancel out of this procedure, and assign the policy at a later time.
- 9 In the Assign LiveUpdate Policy dialog box, check one or more groups to which to assign this policy, and then click **Assign**.

## Distributing content to managed clients with third party distribution tools

After you configure the LiveUpdate Policy to enable third party content management, you locate and copy the content on Symantec Endpoint Protection Manager. After you locate and copy the content, you distribute it to clients. You also decide what content to copy and distribute.

---

**Note:** If you stage update files on client computers before placing them in the /inbox directory, you must copy the files. Moving the files does not work. You can also copy .vdb and .jdb files to the inbox for processing.

---

### To distribute content to managed clients with third party distribution tools

- 1 On the computer that runs the Symantec Endpoint Protection Manager, create a working directory such as `\Work_Dir`.
- 2 On the console, on the Clients tab, right-click the group to update, and then click **Properties**.
- 3 Document the first four hexadecimal values of the Policy Serial Number, such as 7B86.
- 4 Navigate to the following directory:  
`\\Program Files\Symantec\Symantec Endpoint Protection Manager\data\outbox\agent`
- 5 Locate the directory that contains the first four hexadecimal values that match your client group Policy Serial Number.
- 6 Open that directory, and then copy `index2.dax` to your working directory, such as `\Work_Dir\index2.dax`.
- 7 Navigate to the following directory:  
`\\Program Files\Symantec\Symantec Endpoint Protection Manager\Inetpub\content`
- 8 Open and read `ContentInfo.txt` to discover the content that each <<target moniker>> directory contains.  
  
The contents of each directory is <<target moniker>>\<sequence num>\full.zip|full.  
  
The file that you want is <<target moniker>>\<latest sequence num>\index.dax.
- 9 Copy the content of each <<target moniker>> directory to your working directory such as `\Work_Dir`.

- 10 Delete all files and directories from each \<<target moniker>> so that only the following directory structure and file remain in your working directory:

```
\\Work_Dir\<<target moniker>>\<latest sequence number>\full.zip
```

Your working directory now contains the directory structure and files to distribute to your clients.

- 11 Use your third party distribution tools to distribute the content of \Work\_Dir to the \\Symantec Endpoint Protection\inbox\ directory on your clients in your group.

The end result must look like the following:

```
\\Symantec Endpoint Protection\inbox\index2.dax
```

```
\\Symantec Endpoint Protection\inbox\<<target moniker>>\<latest sequence number>\full.zip
```

If the files disappear so that \inbox\ is empty, you were successful. If an \inbox\invalid\ directory appears, you were not successful and must try again

## About using third party distribution tools to distribute updates to unmanaged clients

If you installed unmanaged clients from the installation CD, the clients do not trust and do not process content or policy updates for security purposes. To enable these clients to process updates, you have to create the following registry key:

```
HKLM\Software\Symantec\Symantec Endpoint Protection\SMC\TPMState
```

Set the value to hexadecimal 80 so that the key looks like 0x00000080 (128)

After you set this key, you must either restart the computer or execute the following commands from the \Symantec\Symantec Endpoint Protection\ directory:

```
smc.exe -stop
```

```
smc.exe -start
```

The following directory appears on the client computers that do not run Windows Vista:

```
\\Documents and Settings\All Users\Application Data\Symantec\Symantec Endpoint Protection\inbox\
```

The following directory appears on the client computers that do run Windows Vista:

```
\\Program Data\Symantec\Symantec Endpoint Protection\inbox\
```

You can now use third party distribution tools to copy content or policy updates to this directory. The Symantec client software then trusts and process the content.

You get the content to distribute from a Symantec Endpoint Protection Manager almost the same way that you do for managed clients.

However, copy index2.xml from the Global group, instead of copying index2.dax from your managed client group directory, as described in step 2 of [“To distribute content to managed clients with third party distribution tools”](#) on page 100. Copy the full.dax file as described for the managed client. You can then distribute these files. You can also drop .vdb and .jdb files in the client inbox for processing.

---

**Note:** If you stage the update files on the computers, you must copy them to the inbox. The update files are not processed if you move them to the inbox.

---

See [“Distributing content to managed clients with third party distribution tools”](#) on page 99.

---

**Note:** After a managed client installation, the TPMState registry key exists with a value of 0, which you can change. (This key does not exist after an unmanaged client installation.) Also, restarting the computer or smc.exe command execution is not required for a managed client installation. The directory appears as soon as the registry key is changed.

---

# Limiting user access to client features

This chapter includes the following topics:

- [About access to the client interface](#)
- [Locking and unlocking managed settings](#)
- [Changing the user control level](#)
- [Password-protecting the client](#)

## About access to the client interface

You can determine the level of interaction that you want users to have on the Symantec Endpoint Protection client. Choose which features are available for users to configure. For example, you can control the number of notifications that appear and limit users' ability to create firewall rules and antivirus scans. You can also give users full access to the user interface.

The features that users can customize for the user interface are called managed settings. The user does not have access to all the client features, such as password protection.

To determine the level of user interaction, you can customize the user interface in the following ways:

- For antivirus and antispyware settings, you can lock or unlock the settings.
- For firewall settings, intrusion prevention settings, and for some client user interface settings, you can set the user control level and configure the associated settings.
- You can password-protect the client.



See [“Password-protecting the client”](#) on page 109.

## Locking and unlocking managed settings

To determine which Antivirus and Antispyware Protection and Tamper Protection features are available for users to configure on the client, you lock or unlock them. Users can configure unlocked settings, but users cannot configure locked settings. Only administrators on the Symantec Endpoint Protection Manager console can configure locked settings.

[Table 7-1](#) describes the padlock icons.

**Table 7-1** Locked and unlocked padlock icons

Icon	What the icon means
	The setting is unlocked and users can change it in the client user interface. On the client, the padlock icon does not appear and the option is available.
	The setting is locked and users cannot change it in the client user interface. On the client, the locked padlock appears and the option appears dimmed.

You lock and unlock the settings on the pages or dialog boxes where they appear.

### To lock and unlock managed settings

- 1 Open an Antivirus and Antispyware Policy.  
See [“About editing policies”](#) on page 327.
- 2 On the Antivirus and Antispyware page, click one of the following pages:
  - File System Auto-Protect
  - Internet Email Auto-Protect
  - Microsoft Outlook Auto-Protect
  - Lotus Notes Auto-Protect
  - TruScan Proactive Threat Scans
  - Submissions
  - Miscellaneous



- 3 Click the padlock icon to lock or unlock the setting.
- 4 If you are finished with the configuration for this policy, click **OK**.

You can also lock and unlock Tamper Protection settings.

See [“Configuring Tamper Protection”](#) on page 298.

## Changing the user control level

You can determine which Network Threat Protection features and client user interface settings are available for users to configure on the Symantec Endpoint Protection client. To determine which settings are available, you specify the user control level. The user control level determines whether the client can be completely invisible, display a partial set of features, or display a full user interface.

---

**Note:** The Symantec Network Access Control client only runs in server control. Users cannot configure any user interface settings.

---

[Table 7-2](#) displays the Symantec Endpoint Protection client's user control levels.

**Table 7-2** 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"> <li>■ 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 on the Symantec Endpoint Protection Manager console for the client.</li> <li>■ Users can view logs, the client's traffic history, and the list of applications that the client runs.</li> <li>■ 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.</li> </ul> <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>

**Table 7-2** User control levels (*continued*)

User control level	Description
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"> <li>■ Users can configure or enable firewall rules, application-specific settings, firewall notifications, firewall settings, intrusion prevention settings, and client user interface settings.</li> <li>■ The client ignores the firewall rules that you configure for the client.</li> </ul> <p>You can give client control to the client computers that employees use in a remote location or a home location.</p>
Mixed control	<p>Gives the user a mixture of control over the client.</p> <p>Mixed control has the following characteristics:</p> <ul style="list-style-type: none"> <li>■ Users can configure the firewall rules and application-specific settings.</li> <li>■ 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.</li> <li>■ 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.</li> <li>■ You can configure Antivirus and Antispyware Protection settings to override the setting on the client, even if the setting is unlocked. For example, if you unlock the Auto-Protect feature and the user disables it, you can enable Auto-Protect.</li> </ul> <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> <p>See <a href="#">“About mixed control”</a> on page 107.</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.

You can set a different user control level for each location.

---

**Note:** Clients that run in client control or mixed control switch to server control when the server applies a Quarantine Policy.

---

#### To change the user control level

- 1 In the console, click **Clients**.
- 2 Under View Clients, select the group whose location you want to modify.
- 3 Click the **Policies** tab.
- 4 Under Location-specific Policies and Settings, under the location you want to modify, expand **Location-specific Settings**.
- 5 To the right of Client User Interface Control Settings, click **Tasks > Edit Settings**.
- 6 In the Client User Interface Control Settings dialog box, do one of the following options:
  - Click **Server control**, and then click **Customize**.  
Configure any of the settings, and then click **OK**.
  - Click **Client control**.
  - Click **Mixed control**, and then click **Customize**.  
Configure any of the settings, and then click **OK**.  
See [“About mixed control”](#) on page 107.
  - For the Symantec Network Access Control client, you can click **Display the client** and **Display the notification area icon**.
- 7 Click **OK**.

## About mixed control

For clients in mixed control, you can determine which managed options you want users to configure or not. Managed options include settings in a Firewall Policy, an Intrusion Prevention Policy, and the client user interface settings.

For each option, you can assign it to server control or you can assign it to client control. In client control, only the user can enable or disable the setting. In server control, only you can enable or disable the setting. Client control is the default user control level. If you assign an option to server control, you then configure the setting in the corresponding page or dialog box in the Symantec Endpoint Protection Manager console. For example, you can enable the firewall settings in

the Firewall Policy. You can configure the logs in the Client Log Settings dialog box on the Policies tab of the Clients page.

You can configure the following types of settings:

- User interface settings
- General Network Threat Protection settings
- Firewall Policy settings
- Intrusion Prevention Policy settings

## Configuring user interface settings

You can configure user interface settings on the client if you do either of the following tasks:

- Set the client's user control level to server control.
- Set the client's user control level to mixed control and set the parent feature on the Client/Server Control Settings tab to Server.  
For example, you can set the Show/Hide notification area icon option to Client. The notification area icon appears on the client and the user can choose to show or hide the icon. If you set the Show/Hide notification area icon option to Server, you can choose whether to display the notification area icon on the client.

### To configure user interface settings in mixed control

- 1 Change the user control level to mixed control.  
See [“Changing the user control level”](#) on page 105.
- 2 In the Client User Interface Control Settings for *location name* dialog box, next to Mixed control, click **Customize**.
- 3 In the Client User Interface Mixed Control Settings dialog box, on the Client/Server Control Settings tab, do one of the following actions:
  - Lock an option so that you can configure it only from the server. For the option you want to lock, click **Server**.  
Any Antivirus and Antispyware Protection settings that you set to Server here override the settings on the client.
  - Unlock an option so that the user can configure it on the client. For the option you want, click **Client**. Client is selected by default for all settings except the antivirus and antispyware settings.

- 4 For the following options that you set to Server, click the **Client User Interface Settings** tab to configure them:

Show/Hide notification area icon	Display the notification area icon
Enable/Disable Network Threat Protection	Allow users to enable and disable Network Threat Protection
Test Network Security menu command	Allow users to perform a security test
Show/Hide Intrusion Prevention Notifications	Display Intrusion Prevention notifications

For information on where in the console you configure the remaining options that you set to Server, click **Help**. To enable firewall settings and intrusion prevention settings, configure them in the Firewall Policy and Intrusion Prevention Policy.

See [“Enabling Smart traffic filtering”](#) on page 443.

See [“Enabling traffic and stealth settings”](#) on page 444.

See [“Configuring intrusion prevention”](#) on page 449.

- 5 On the Client User Interface Settings tab, check the option's check box so that the option is available on the client.
- 6 Click **OK**.
- 7 Click **OK**.

#### To configure user interface settings in server control

- 1 Change the user control level to mixed control.  
See [“Changing the user control level”](#) on page 105.
- 2 In the Client User Interface Control Settings for *location name* dialog box, next to Server control, click **Customize**.
- 3 In the Client User Interface Settings dialog box, check an option's check box so that the option appears on the client for the user to use.
- 4 Click **OK**.
- 5 Click **OK**.

## Password-protecting the client

You can increase corporate security by requiring password protection on the client computer whenever users perform certain tasks.

You can require the users to type a password when users try to do one of the following actions:

- Open the client's user interface.
- Stop the client.
- Import and export the security policy.
- Uninstall the client.

You can modify password protection settings only for the subgroups that do not inherit from a parent group.

#### **To password-protect the client**

- 1 In the Symantec Endpoint Protection Manager console, click **Clients**.
- 2 Under View Clients, select the group for which you want to set up password protection.
- 3 On the Policies tab, under Location-independent Policies and Settings, click **General Settings**.
- 4 Click **Security Settings**.
- 5 On the Security Settings tab, choose any of the following check boxes:
  - Require a password to open the client user interface
  - Require a password to stop the client service
  - Require a password to import or export a policy
  - Require a password to uninstall the client
- 6 In the Password text box, type the password.  
The password is limited to 15 characters or less.
- 7 In the Confirm password text box, type the password again.
- 8 Click **OK**.

# Setting up connections between management servers and clients

This chapter includes the following topics:

- [About management servers](#)
- [Specifying a management server list](#)
- [Adding a management server list](#)
- [Assigning a management server list to a group and location](#)
- [Viewing the groups and locations to which a management server list is assigned](#)
- [Editing the server name and description of a management server list](#)
- [Editing the IP address, host name, and port number of a management server in a management server list](#)
- [Changing the order in which management servers connect](#)
- [Replacing a management server list](#)
- [Copying and pasting a management server list](#)
- [Exporting and importing a management server list](#)
- [Deleting a management server list](#)
- [About client and server communication settings](#)

## About management servers

Clients and Enforcers must be able to connect to management servers to download security policies and settings. The Symantec Endpoint Protection Manager includes a file that helps manage the traffic between clients, management servers, and optional Enforcers. The file specifies to which management server a client or Enforcer connects. It can also specify to which management server a client or Enforcer connects in case of a management server's failure.

This file is referred to as a management server list. A management server list includes the management server's IP addresses or host names to which clients and optional Enforcers can connect after the initial installation. You can customize the management server list before you deploy any clients or optional Enforcers.

When the Symantec Endpoint Protection Manager is installed, a default management server list is created to allow for HTTP communication between clients, Enforcers, and management servers. The default management server list includes the IP addresses of all connected network interface cards (NICs) on all of the management servers at the site.

You may want to include only the external NICs in the list. Although you cannot edit the default management server list, you can create a customized management server list. A custom management server list includes the exact management servers and the correct NICs to which you want clients to connect. In a customized list, you can also use HTTPS protocol, verify the server certificate, and customize the HTTP or HTTPS port numbers.

## Specifying a management server list

You can specify a list of management servers to connect to a group of clients and optional Enforcers at any time. However, you typically perform this task after you have created a custom management server list and before you deploy any client packages.

### To specify a management server list

- 1 In the Symantec Endpoint Protection Manager console, click **Clients**.
- 2 On the Clients page, under View Clients, select the group for which you want to specify a management server list.
- 3 On the Policies tab, uncheck **Inherit policies and settings from parent group**.  
You cannot set any communication settings for a group unless the group no longer inherits any policies and settings from a parent group.
- 4 Under Location-independent Policies and Settings, in the Settings area, click **Communication Settings**.



- 5 In the Communication Settings for *group name*, under Management Server List, select the management server list.

The group that you select then uses this management server list when communicating with the management server.

- 6 Click **OK**.

## Adding a management server list

If your enterprise has multiple Symantec Endpoint Protection Managers, you can create a customized management server list. The management server list specifies the order in which clients in a particular group connect. Clients and optional Enforcers first try to connect to management servers that have been added with the highest priority.

If management servers with the highest priority are not available, then clients and optional Enforcers try to connect to management servers with the next higher priority. A default management server list is automatically created for each site. All available management servers at that site are added to the default management server list with the same priority.

If you add multiple management servers at the same priority, then clients and optional Enforcers can connect to any of the management servers. Clients automatically balance the load between available management servers at that priority.

You can use HTTPS protocol rather than the default HTTP for communication. If you want to secure communication further, you can customize the HTTP and HTTPS port numbers by creating a customized management server list. However, you must customize the ports before clients are installed or else the client-to-management server communication is lost. If you update the version of the Symantec Endpoint Protection Manager, you must remember to re-customize the ports so that the clients can resume communication.

After you add a new management server list, you must assign it to a specific group or location or both.

See [“Assigning a management server list to a group and location”](#) on page 114.

### To add a management server list

- 1 In the Symantec Endpoint Protection Manager console, click **Policies**.
- 2 In the Policies page, under View Policies, click **Policy Components > Management Server Lists**.
- 3 Under Tasks, click **Add a Management Server List**.

- 4 In the Management Server Lists dialog box, in the Name text field, type a name for the management server list and an optional description.
- 5 To specify which communication protocol to use between the management servers and the clients and Enforcers, select one of the following options:
  - Use HTTP protocol
  - Use HTTPS protocol  
Use this option if you want management servers to communicate by using HTTPS and if the server is running Secure Sockets Layer (SSL).
- 6 If you require verification of a certificate with a trusted third-party certificate authority, check **Verify certificate when using HTTPS protocol**.
- 7 To add a server, click **Add > New Server**.
- 8 In the Add Management Server dialog box, in the Server address text field, type the IP address or host name of the management server.
- 9 If you want to change the port number for either the HTTP or HTTPS protocol for this server, do one of the following tasks:
  - Check **Customize HTTP port number** and enter a new port number.  
The default port number for the HTTP protocol is 80.
  - Check **Customize HTTPS port number** and enter a new port number.  
The default port number for the HTTPS protocol is 443.  
If you customize the HTTP or HTTPS port numbers after client deployment, clients lose communication with the management server.
- 10 Click **OK**.
- 11 If you need to add a management server that has a different priority than the management server you just added, click **Add > New Priority**.
- 12 Repeat steps 7 through 10 to add more management servers.
- 13 In the Management Server Lists dialog box, click **OK**.

## Assigning a management server list to a group and location

After you add a policy, you need to assign it to a group or a location or both. Otherwise the management server list is not effective. You must have finished adding or editing a management server list before you can assign the list.

See [“Adding a management server list”](#) on page 113.

See “[Editing the server name and description of a management server list](#)” on page 116.

See “[Editing the IP address, host name, and port number of a management server in a management server list](#)” on page 116.

#### To assign a management server list to a group and location

- 1 In the Symantec Endpoint Protection Manager console, click **Policies**.
- 2 In the Policies page, under View Policies, click **Policy Components > Management Server Lists**.
- 3 In the Management Server Lists pane, select the management server list you want to assign.
- 4 Under Tasks, click **Assign the List**.
- 5 In the Apply Management Server List dialog box, check the groups and locations to which you want to apply the management server list.
- 6 Click **Assign**.
- 7 When you are prompted, click **Yes**.

## Viewing the groups and locations to which a management server list is assigned

You may want to display the groups and locations to which a management server list has been assigned.

#### To view the groups and locations to which a management server list is assigned

- 1 In the Symantec Endpoint Protection Manager console, click **Policies**.
- 2 On the Policies page, under View Policies, click **Policy Components > Management Server Lists**.
- 3 In the Management Server Lists pane, select the management server list whose groups and locations you want to display.
- 4 Under Tasks, click **Show the Assigned Groups or Locations**.  
The groups or locations that are assigned the selected management server list display a small green circle with a white check mark.
- 5 In the *management server list name*: Assigned Groups & Locations dialog box, click **OK**.

## Editing the server name and description of a management server list

You can change the name and description of a management server list.

See [“Assigning a management server list to a group and location”](#) on page 114.

**To edit the server name and description of a management server list**

- 1 In the Symantec Endpoint Protection Manager console, click **Policies**.
- 2 On the Policies page, under View Policies, click **Policy Components > Management Server Lists**.
- 3 In the Management Server Lists pane, select the management server list whose name and description you want to modify.
- 4 Under Tasks, click **Edit the List**.
- 5 In the Management Server Lists dialog box, edit the name and optional description of the management server list.
- 6 Click **OK**.

## Editing the IP address, host name, and port number of a management server in a management server list

If the IP address or host name of a management server changes, you need to change it in the management server list. You can also change the port number for the HTTP or HTTPS communication protocol.

See [“Assigning a management server list to a group and location”](#) on page 114.

**To edit the IP address, host name, and port number of a management server in a management server list**

- 1 In the Symantec Endpoint Protection Manager console, click **Policies**.
- 2 On the Policies page, under View Policies, click **Policy Components > Management Server Lists**.
- 3 In the Management Server Lists pane, select the management server list that you want to modify.
- 4 Under Tasks, click **Edit the List**.
- 5 In the Management Server Lists dialog box, select the management server that you want to modify.
- 6 Click **Edit**.

- 7 In the Add Management Server dialog box, type the new IP address or host name of the management server in the Server address box.  
You can also change the port number for the HTTP or HTTPS protocol.
- 8 Click **OK**.
- 9 In the Management Server Lists dialog box, click **OK**.

## Changing the order in which management servers connect

If circumstances change in a network, you may need to reassign IP addresses or host names, as well as priorities in a management server list. For example, one of the servers on which you installed the Symantec Endpoint Protection Manager had a disk failure. This management server had served as a load balancing server and had been assigned Priority 1. However, you have another management server with an assigned Priority 2. If you want to resolve this problem, you can reassign the priority of this management server. You can assign a management server's priority from 2 to 1 to replace the defective management server.

### To change the order in which management servers connect

- 1 In the Symantec Endpoint Protection Manager console, click **Policies**.
- 2 On the Policies page, under View Policies, click **Policy Components > Management Server Lists**.
- 3 In the Management Server Lists pane, select the management server list for which you want to change the order of the management servers.
- 4 Under Tasks, click **Edit the List**.
- 5 In the Management Server Lists dialog box, under Management Servers, select the IP address, host name, or priority of the management server.  
You can move an IP address or a host name to a different priority. If you decide to change a priority, it also automatically changes the priority of all of the associated IP addresses and host names.
- 6 Click **Move Up** or **Move Down**.
- 7 In the Management Server Lists dialog, click **OK**.

## Replacing a management server list

You may want to replace a management server list that has previously been applied to a specific group or location with another one.

#### To replace a management server list

- 1 In the Symantec Endpoint Protection Manager console, click **Policies**.
- 2 On the Policies page, under View Policies, click **Policy Components > Management Server Lists**.
- 3 In the Management Server Lists pane, select the management server list that you want to replace.
- 4 Under Tasks, click **Replace the List**.
- 5 In the Replace Management Server List dialog box, select the replacement management server list from the New Management Server drop-down list.
- 6 Check the groups or locations to which you want to apply the replacement management server list.
- 7 Click **Replace**.
- 8 When you are prompted, click **Yes**.

## Copying and pasting a management server list

You may want multiple management lists that are nearly identical, except for a few changes. You can make a copy of a management server list. After you copied and pasted a management server list, the copy of the management server list appears in the Management Server Lists pane.

#### To copy and paste a management server list

- 1 In the Symantec Endpoint Protection Manager console, click **Policies**.
- 2 On the Policies page, under View Policies, click **Policy Components > Management Server Lists**.
- 3 In the Management Server Lists pane, select the management server list that you want to copy.
- 4 Under Tasks, click **Copy the List**.
- 5 Under Tasks, click **Paste List**.

## Exporting and importing a management server list

You may want to export or import an existing management server list. The file format for a management server list is: .dat

**To export a management server list**

- 1 In the Symantec Endpoint Protection Manager console, click **Policies**.
- 2 On the Policies page, under View Policies, click **Policy Components > Management Server Lists**.
- 3 In the Management Server Lists pane, select the management server list that you want to export.
- 4 On the Policies page, under Tasks, click **Export the List**.
- 5 In the Export Policy dialog box, browse for the folder into which you want to export the management server list file.
- 6 Click **Export**.
- 7 If you are prompted to change the file name in the Export Policy dialog, modify the file name, and then click **OK**.

**To import a management server list**

- 1 In the Symantec Endpoint Protection Manager console, click **Policies**.
- 2 In the Policies page, under View Policies, click **Policy Components > Management Server Lists**.
- 3 Under Tasks, click **Import a Management Server List**.
- 4 In the Import Policy dialog box, browse to the management server list file that you want to import, and then click **Import**.
- 5 If you are prompted to change the file name in the Input dialog box, modify the file name, and then click **OK**.

## Deleting a management server list

You may need to delete a management server list because servers may no longer be operational or your network has been reconfigured.

**To delete a management server list**

- 1 In the Symantec Endpoint Protection Manager console, click **Policies**.
- 2 On the Policies page, under View Policies, click **Policy Components > Management Server Lists**.
- 3 In the Management Server Lists pane, select the management server list that you want to delete.
- 4 On the Policies page, under Tasks, click **Delete the List**.
- 5 In the Delete Management Server List dialog box, click **Yes**.

## About client and server communication settings

The communication settings between the client and server and other client settings are stored in files on the client computer.

[Table 8-1](#) describes the files that are used to store the client user interface state.

**Table 8-1** Client files

File name	Description
SerDef.dat	An encrypted file that stores communication settings by location. Each time the user changes locations, the SerDef.dat file is read and the appropriate communication settings for the new location are applied to the client.
sylink.xml	Stores the global communication settings. This file is for internal use only and should not be edited. It contains settings from the Symantec Endpoint Protection Manager. If you edit this file, most settings will be overwritten by the settings from the Symantec Endpoint Protection Manager the next time the client connects to the Symantec Endpoint Protection Manager.
SerState.dat	An encrypted file that stores information about the GUI, such as screen size, whether the Message Console is displayed, and whether Windows services are displayed. When the client starts, it reads this file and returns to the same GUI state as before it was stopped.



# Reporting basics

This chapter includes the following topics:

- [About reporting](#)
- [About the reports you can run](#)
- [About the display of logs and reports](#)
- [How reporting uses the database](#)
- [About logged events from your network](#)
- [About the logs you can monitor](#)
- [Accessing the reporting functions](#)
- [Associating localhost with the IP address when you have loopback addresses disabled](#)
- [About using SSL with the reporting functions](#)
- [Using the Symantec Endpoint Protection Home page](#)
- [Using the Symantec Network Access Control Home page](#)
- [Configuring reporting preferences](#)
- [About the client scan times used in reports and logs](#)
- [About using the Past 24 hours filter in reports and logs](#)
- [About using the filters that search for groups in reports and logs](#)

## About reporting

The reporting functions give you the up-to-date information that you need to monitor and make informed decisions about the security of your network. The management console Home page displays the automatically generated charts that contain information about the important events that have happened recently in your network. You can use the filters on the Reports page to generate predefined or custom reports. You can use the Reports page to view graphical representations and statistics about the events that happen in your network. You can use the filters on the Monitors page to view more detailed, real-time information about your network from the logs.

If you have Symantec Endpoint Protection installed, reporting includes the following features:

- Customizable Home page with your most important reports, overall security status, and links to Symantec Security Response
- Summary views of reports on antivirus status, Network Threat Protection status, compliance status, and site status
- Predefined quick reports and customizable graphical reports with multiple filter options that you can configure
- The ability to schedule reports to be emailed to recipients at regular intervals
- Support for Microsoft SQL or an embedded database for storing event logs
- The ability to run client scans, to turn on the client Network Threat Protection and Auto-Protect, and to restart computers directly from the logs
- The ability to add application exclusions directly from the logs
- Configurable notifications that are based on the security events

If you have Symantec Network Access Control installed, reporting includes the following features:

- Home page with an overall summary view of compliance status
- Predefined and customizable graphical reports with multiple filter options
- Support for Microsoft SQL or an embedded database for storing event logs
- The ability to schedule reports to be emailed to recipients at regular intervals
- Configurable notifications that are based on the security events

Reporting runs as a Web application within the management console. The application uses a Web server to deliver this information. You can also access reporting functions from a stand-alone Web browser that is connected to your management server.

Basic reporting tasks include the following:

- Logging on to reporting by using a Web browser
- Using the Home page and summary view to get quick information about events in your security network
- Configuring your reporting preferences
- Using links to Symantec Security Response

## About the reports you can run

Symantec Endpoint Protection and Symantec Network Access Control collect information about the security events in your network. You can view predefined quick reports, and you can generate custom reports that are based on the filter settings you select. You can also save filter configurations to generate the same custom reports in the future and delete them when they are no longer needed.

[Table 9-1](#) describes the types of reports that are available.

**Table 9-1** Report types

Report type	Description
Application and Device Control	Displays information about events where some type of behavior was blocked. These reports include information about application security alerts, blocked targets, and blocked devices. Blocked targets can be registry keys, dlls, files, and processes.
Audit	Displays information about the policies that clients and locations use currently.
Compliance	Displays information about the compliance status of your network. These reports include information about Enforcer servers, Enforcer clients, Enforcer traffic, and host compliance.
Computer Status	Displays 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 information about intrusion prevention, attacks on the firewall, and about firewall traffic and packets.

**Table 9-1** Report types (*continued*)

Report type	Description
Risk	Displays information about risk events on your management servers and their clients. It includes information about TruScan proactive threat scans.
Scan	Displays information about antivirus and antispyware scan activity.
System	Displays information about event times, event types, sites, domains, servers, and severity levels.

See [“About reports”](#) on page 148.

---

**Note:** Some predefined reports contain information that is obtained from Symantec Network Access Control. If you have not purchased that product, but you run one of that product's reports, the report is empty.

---

You can modify the predefined reports and save your configuration. You can create new filter configurations that are based on a predefined configuration or on an existing custom configuration that you created. You can also delete your customized configurations if you don't need them anymore. The active filter settings are listed in the report if you have configured the log and report preferences setting to include the filters in reports.

See [“Configuring logs and reports preferences”](#) on page 142.

When you create a report, the report appears in a separate window. You can save a copy of the report in Web archive format or you can print a copy of the report. The saved file or printed report provides a snapshot of the current data in your reporting database so that you can retain a historical record.

You can also create scheduled reports that are automatically generated based on a schedule that you configure. You set the report filters and the time to run the report. When the report is finished, it is emailed to one or more recipients.

A scheduled report always runs by default. You can change the settings for any scheduled report that has not yet run. You can also delete a single scheduled report or all of the scheduled reports.

See [“Creating and deleting scheduled reports”](#) on page 168.

## About the display of logs and reports

The optimal display resolution for reporting functions is 1024 x 768 or higher. However, you can view the reporting functions with a screen resolution as low as 800 x 600 by using the scroll bars.

## How reporting uses the database

Symantec Endpoint Protection collects and reads the events that occur in your network from the management server logs stored in the database. The database can be an existing Microsoft SQL database in your network or the embedded database that is installed with the reporting software.

The database has a few reporting-related maintenance requirements.

See “[About managing log events in the database](#)” on page 282.

You can obtain the database schema that Symantec Endpoint Protection uses if you want to construct your own reports by using third-party software. For information about the database schema, see the Symantec Knowledge Base.

## About logged events from your network

Symantec Endpoint Protection pulls the events that appear in the reports from the event logs on your management servers. The event logs contain time-stamps in the clients' time zones. When the management server receives the events, it converts the event time-stamps to Greenwich Mean Time (GMT) for insertion into the database. When you create reports, the reporting software displays information about events in the local time of the computer on which you view the reports.

Some types of events such as virus outbreaks can result in an excessive number of security events being generated. These types of events are aggregated before they are forwarded to the management server.

For information about the events that appear on the Home page, see the Symantec Security Response Web site Attack Signatures page. On the Internet, go to the following URL:

[http://securityresponse.symantec.com/avcenter/attack\\_sigs/](http://securityresponse.symantec.com/avcenter/attack_sigs/)

## About the logs you can monitor

You can look at event data directly if you want to focus on specific events. Logs include event data from your management servers as well as all of the clients that report to those servers.

You can filter the log data in the same way as you can filter report data. You can export log data to a comma-separated file and can export some data to a text file or to a Syslog server. This capability is useful to back up the event data or when you want to use the data in a spreadsheet or other application.

See [“Exporting log data”](#) on page 189.

## Accessing the reporting functions

Reporting runs as a Web application within the management console. The application uses a Web server to deliver this information. You can access the reporting functions, which are located on the Home page, Monitors page, and Reports page, from the console.

You can also access the Home, Monitors, and Reports page functions from a stand-alone Web browser that is connected to your management server. You can perform all the reporting functions from either the console or a stand-alone Web browser. However, all of the other console functions are not available when using a stand-alone browser.

To access reporting from a Web browser, you must have the following information:

- The IP address or host name of the management server.
- The account name and password for the manager.

When you use a Web browser to access reporting functions, no pages or page icons are in the display. All the tabs that are located on the Home, Monitors, and Reports console pages are located across the top of the browser window.

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.

---

**Note:** To access the reporting functions by either method, you must have Internet Explorer 6.0 or later installed. Other Web browsers are not supported.

---

The information that is given here assumes that you use the management console to access reporting functions rather than a Web browser. Procedures for using reporting are similar regardless of how you access reporting. However, procedures specifically using reporting in a stand-alone browser are not documented, except for how to log on using a stand-alone Web browser.

---

**Note:** You can also use the console or a Web browser to view reports when logged in through a remote terminal session.

---

See “[Logging on to the Symantec Endpoint Protection Manager](#)” on page 29.

Context-sensitive Help is available by clicking the Tell me more link, which is located on the console pages that are used for reporting functions.

---

**Note:** If you do not use the default port when you install the Help pages for reporting, you cannot access the on-line context-sensitive Help. To access context-sensitive Help when you use a non-default port, you must add a variable to the Reporter.php file.

---

#### To log on to reporting from a stand-alone Web browser

- 1 Open a Web browser.
- 2 Type the reporting URL into the address text box in the format that follows:  
**`http://server name /reporting/index.php?`**
- 3 When the logon dialog box appears, type your user name and password, and then click **Log On**.

If you have more than one domain, in the Domain text box, you need to type your domain name.

#### To change the port used to access context-sensitive Help for reporting

- 1 Change directory to *drive*:\Program Files\Symantec\Symantec Endpoint Protection Manager\Inetpub\Reporting\Resources.
- 2 Open the Reporter.php configuration file with an editor.
- 3 Add the following line to the file, and replace *port number* with the port number you used when you installed reporting Help.  
**`$scm_http_port=port number`**
- 4 Save and close the file.

## Associating localhost with the IP address when you have loopback addresses disabled

If you have disabled loopback addresses on the computer, the reporting pages do not display. If you try to log on to the management 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 Reporting 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.

#### 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 management console computer
```

- 4 Save and close the file.

## About using SSL with the reporting functions

You can use SSL with the reporting functions for increased security. SSL provides confidentiality, the integrity of your data, and authentication between the client and the server.

For information about using SSL with the reporting functions, see "Configuring SSL to work with the Symantec Endpoint Protection reporting functions" in the Symantec Knowledge Base at the following URL:

<http://service1.symantec.com/SUPPORT/ent-security.nsf/docid/2007072512593748>

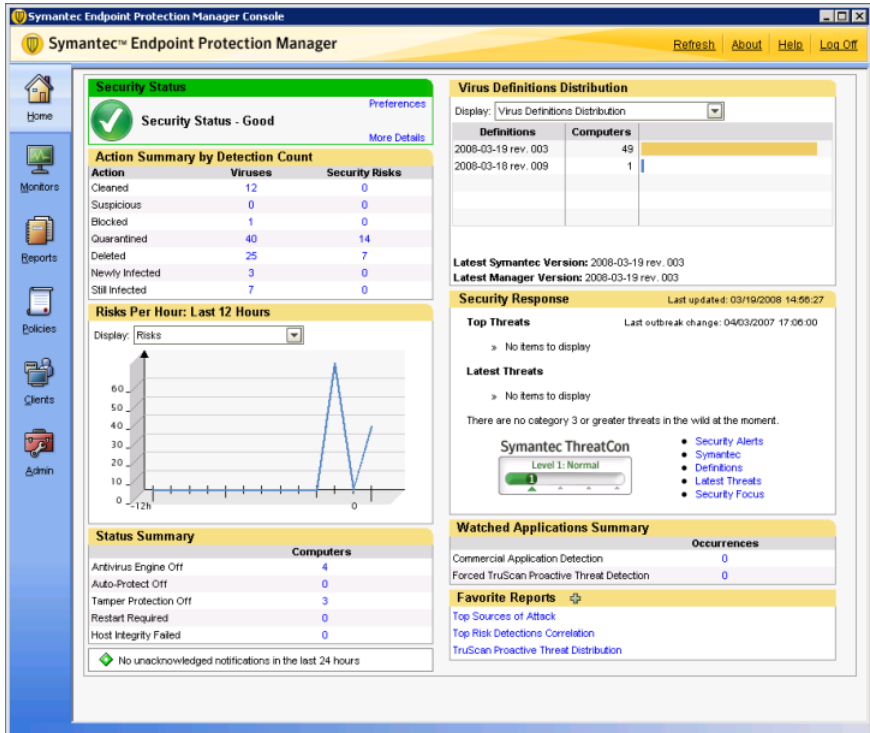
## Using the Symantec Endpoint Protection Home page

If you have Symantec Endpoint Protection installed and your administrator account rights include permission to view reports, then your Home page displays automatically generated reports. These reports contain important information about your network security. If you do not have permission to view reports, your Home Page does not contain these automatically generated reports.



Figure 9-1 shows a sample Home page that the administrators that have permission to view reports see.

Figure 9-1 Sample Symantec Endpoint Protection Home page on the console



The Home page includes automatically generated reports and several status items. Some of the Home page reports are hyperlinked to more detailed reports. You can click on the numbers and some charts in the Home page reports to see details.

**Note:** Reports are filtered automatically based on the permissions of the user who is logged on. If you are a system administrator, you see information across domains. If you are a limited administrator with access rights to only one domain, you see information from only that one domain.

Table 9-2 describes each item on the Symantec Endpoint Protection Home page in detail.

**Table 9-2** Home page items and reports

Report or Status Information	Description
Security Status	<p>Security Status can be either Good or Attention Needed. The thresholds that you set on the Security status tab determine the definitions of Good and Attention Needed. You access the Security status tab from the Preferences link on the Home page.</p> <p>See <a href="#">“Configuring security status thresholds”</a> on page 141.</p> <p>You can click the security status icon on the Home page for details.</p>

**Table 9-2** Home page items and reports (*continued*)

Report or Status Information	Description
<p><i>Action Summary by Detection Count</i>    <i>Action Summary by Number of Computers</i></p>	<p>By default, the Home Page displays an action summary for the last 24 hours and by the infection count for viruses and security risks. You can click the Preferences link to change the time interval that is used to the past week instead of the past 24 hours. You can use the same link to change the display by Detection Count to a display by the Number of Computers.</p> <p>See <a href="#">“About Home and Monitors display options”</a> on page 140.</p> <p>The Action Summary by Detection Count summarizes the following information:</p> <ul style="list-style-type: none"> <li>■ A count of the actions that have been taken on viruses and security risks.</li> <li>■ The incidence of new virus and security risk detections.</li> <li>■ The number of computers that remain infected by viruses and security risks.</li> </ul> <p>The Action Summary by Number of Computers summarizes the following information:</p> <ul style="list-style-type: none"> <li>■ The number of distinct computers on which the various actions have been performed on viruses and security risks.</li> <li>■ The total number of new virus and security risk detections.</li> <li>■ The total number of computers that still remain infected by viruses and security risks.</li> </ul> <p>For example, suppose you have five Cleaned actions in the Detection Count view. If all of the detections occur on the same computer, then the Number of Computers view shows a count of one, not five.</p> <p>For any of the actions, click the number of viruses or security risks to see a detailed report.</p> <p>A suspicious security risk indicates that a TruScan proactive threat scan has detected something that you should investigate. It may or may not be harmless. If you determine that this risk is harmless, you can use the Centralized Exceptions Policy to exclude it from detection in the future. If you have configured TruScan proactive threat scans to log, and you determine that this risk is harmful, you can use the Centralized Exceptions Policy to terminate or quarantine it. If you have used the default TruScan proactive threat scan settings, then Symantec Endpoint Protection cannot remediate this risk. If you determine that this risk is harmful, you should remove the risk manually.</p>

**Table 9-2** Home page items and reports (*continued*)

Report or Status Information	Description
<p><i>Action Summary by Detection Count</i>    <i>Action Summary by Number of Computers</i>  (Continued)</p>	<p>The Newly Infected count shows the number of risks that have infected computers during the selected time interval only. Newly Infected is a subset of Still Infected. The Still Infected count shows the total number of risks that a scan would continue to classify as infected, also within the configured time interval. For example, computer may still be infected because Symantec Endpoint Protection can only partially remove the risk. After you investigate the risk, you can clear the Still Infected count from the Computer Status log.</p> <p>Both the Newly Infected count and the Still Infected count show the risks that require you to take some further action to clean. In most cases, you can take this action from the console and do not have to go to the computer.</p> <p><b>Note:</b> A computer is counted as part of the Newly Infected count if the detection event that occurred during the time range of the Home page. For example, if an unremediated risk affected a computer within the past 24 hours, the Newly Infected count goes up on the Home page. The risk can be unremediated because of a partial remediation or because the security policy for that risk is set to Log Only.</p> <p>You can configure a database sweep to remove or retain the detection events that resulted in unremediated risks. If the sweep is configured to remove the unremediated risk events, then the Home page count for Still Infected no longer contains those events. Those events age out and are dropped from the database. This disappearance does not mean that the computers have been remediated.</p> <p>No time limit applies to Still infected entries. After you clean the risks, you can change the infected status for the computer. Change the status in the Computer Status log by clicking the icon for that computer in the Infected column.</p> <p><b>Note:</b> The Newly Infected count does not decrement when a computer's infection status is cleared in the Computer Status log; the Still Infected count does decrement.</p> <p>You can determine the total number of events that have occurred in the last time period configured to show on the Home page. To determine total number, add the counts from all rows in the Action Summary except for Still Infected. See "<a href="#">Viewing logs</a>" on page 180.</p>

**Table 9-2** Home page items and reports (*continued*)

Report or Status Information	Description
<p><i>Attacks   Risks   Infections Per Hour: Last 12 Hours   Per Hour: Last 24 Hours</i></p>	<p>This report consists of a line graph. The line graph demonstrates the incidence of either the attacks, detections, or infections in your security network over the last 12 hours or 24 hours. You can select one of the following choices to display:</p> <ul style="list-style-type: none"> <li>■ Attacks represent the incidents that Network Threat Protection thwarted.</li> <li>■ Risks represent all the antivirus, antispymware, and TruScan proactive threat scan detections that were made.</li> <li>■ Infections represent the viruses and security risks that were detected, but cannot be properly remediated.</li> </ul> <p>You can change the display by clicking a new view in the list box.</p> <p><b>Note:</b> You can click the Preferences link to change the default time interval that is used.</p> <p>See <a href="#">“About Home and Monitors display options”</a> on page 140.</p>
<p>Notification status summary</p>	<p>The Notification status summary shows a one-line summary of the status of the notifications that you have configured. For example, 100 unacknowledged notifications in the last 24 hours.</p> <p>See <a href="#">“Creating administrator notifications”</a> on page 195.</p>
<p>Status Summary</p>	<p>The Status Summary summarizes the operational state of the computers in your network. It contains the number of computers in the network that have the following problems:</p> <ul style="list-style-type: none"> <li>■ The Antivirus Engine is turned off.</li> <li>■ Auto-Protect is turned off.</li> <li>■ Tamper Protection is turned off.</li> <li>■ The computers require a restart to complete some form of risk remediation or to complete the installation of a LiveUpdate software download.</li> <li>■ The computers have failed a host integrity check. This number is always zero if you do not have Symantec Network Access Control installed.</li> </ul> <p>You can click each number in the Status Summary for details.</p> <p>The number of unacknowledged notifications in the last 24 hours also appears.</p>
<p><i>Virus Definitions Distribution   Intrusion Prevention Signatures</i></p>	<p>The Virus Definitions Distribution and Intrusion Prevention Signatures section of the Home page shows how the current virus definitions and IPS signatures are distributed.</p> <p>You can toggle between them by clicking a new view in the list box.</p>

**Table 9-2** Home page items and reports (*continued*)

Report or Status Information	Description
Security Response	<p>The Security Response section shows the Top Threats and the Latest Threats as determined by Symantec Security Response. It also shows the number of computers in your network that are unprotected from these threats. The ThreatCon meter indicates the current severity level of threat to computers in a network. The severity levels are based on the threat assessments that Symantec Security Response makes. The ThreatCon severity level provides an overall view of global Internet security.</p> <p>You can click any of the links to get additional information.</p> <p>See <a href="#">“About using Security Response links”</a> on page 136.</p> <p><b>Note:</b> Symantec does not support the installation of the Symantec Client Firewall on the same computer as the Symantec Endpoint Protection Manager. If you install both on the same computer, this situation can cause CGI errors when you click the Security Response links on the Home page.</p>
Watched Applications Summary	<p>The Watched Applications Summary shows the occurrences of applications in your network that are on the following lists:</p> <ul style="list-style-type: none"> <li>■ The Symantec Commercial Applications list</li> <li>■ The Forced TruScan Proactive Threat Detection list, which is your custom list of watched applications</li> </ul> <p>You can click a number to display a more detailed report.</p>
Favorite Reports	<p>The Favorite Reports section contains three default reports. You can customize this section by replacing one or more of these reports with any other default report or custom report that you want. Favorite reports run every time you view them so that their data is current. They display in a new window.</p> <p>To select the reports that you want to access from the Home page, you can click the plus icon beside Favorite Reports.</p>

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

## Configuring the Favorite Reports on the Home page

You can configure the Favorite Reports section on the Home page to provide links to up to three reports that you want to see regularly. You can use this feature to display the reports that you want to see most frequently, every time you log on

to the management console. The Favorite Reports run every time you view them, so they display current information about the state of your network.

The following reports appear in Favorite Reports by default:

- Top Sources of Attack
- Top Risk Detections Correlation
- TruScan Proactive Threat Distribution

---

**Note:** When you customize the display, you customize the display for the currently logged-on user account only.

---

The settings that you configure on this page are saved across sessions. The next time you log on to the management console with the same user credentials, these settings are used for the Home page display.

[Table 9-3](#) describes the Home page display options.

**Table 9-3** Home page favorite reports display options

Option	Definition
Report Type	Specifies the types of reports that are available. Symantec Endpoint Protection provides the following types of reports: <ul style="list-style-type: none"><li>■ Application and Device Control</li><li>■ Audit</li><li>■ Compliance</li><li>■ Computer Status</li><li>■ Network Threat Protection</li><li>■ Risk</li><li>■ Scan</li><li>■ System</li></ul>
Report Name	Lists the names of the reports available for the type of report you selected.
Filter	If you have saved filters associated with the report you selected, they appear in this list box. The default filter is always listed.

#### To configure the favorite reports on the Home page

- 1 Click **Home**.
- 2 Click the plus icon beside **Favorite Reports**.

- 3 From the list box of the report that you want to change, click a report type. For example, click **Risk**.
- 4 From the next list box, click the report name you want. For example, click **Risk Distribution Over Time**.
- 5 If you have saved filters associated with the report you selected, select the one you want to use or select the default filter.
- 6 Repeat for the second and third report links, if desired.
- 7 Click **OK**.

Links to the reports that you selected appear on your Home page.

## About using Security Response links

The Home page includes a summary that is based on the information from the Symantec Security Response Web site. The ThreatCon level severity chart appears as well as links to the Symantec Security Response Web site and other security Web sites. The ThreatCon level shows the condition of the Internet during the last 24 hours. The level is reevaluated every 24 hours unless Internet activity is such that it needs to be done sooner.

The ThreatCon levels are as follows:

■ 1 - Normal

No discernible network incident activity and no malicious code activity with a moderate or severe risk rating. Under Normal conditions, only a routine security posture, designed to defeat normal network threats, is needed. Automated systems and notification mechanisms should be used.

■ 2 - Elevated

The knowledge or the expectation of attack activity is present, without the occurrence of specific events. This rating is used when malicious code reaches a moderate risk rating. Under this condition, a careful examination of vulnerable and exposed systems is appropriate. Security applications should be updated with new signatures and rules as soon as they become available. The careful monitoring of logs is recommended, but no change to actual security infrastructure is required.

■ 3 - High

This level applies when an isolated threat to the computing infrastructure is currently underway or when malicious code reaches a severe risk rating. Under this condition, increased monitoring is necessary. Security applications should be updated with new signatures and rules as soon as they become available. The redeployment and reconfiguration of security systems is recommended.

■ 4 - Extreme



This level applies when extreme global network incident activity is in progress. Implementation of measures in this Threat Condition for more than a short period might create hardship and affect the normal operations of network infrastructure.

For more information about the threat levels, click the Symantec link to display the Symantec Web site.

---

**Note:** Specific security risks are rated from 1 to 5.

---

Each link displays a page in a new window.

[Table 9-4](#) describes the Security Response links.

**Table 9-4** Security Response links on the reporting Home page

Link	What displays
Security Alerts	Displays a summary of the potential threats to your security network that is based on information from Symantec Security Response. The summary includes the latest threats, top threats, and links to removal tools.  You can also search the Symantec Security Response threat database.
Symantec	Displays the Symantec Web site. You can get information about risks and security risks, virus definition downloads, and recent news about Symantec security products.
Definitions	Displays the virus definition download page of the Symantec Web site.
Latest Threats	Displays the Symantec Security Response Web site, which shows the latest threats and security advisories.
Security Focus	Displays the Security Focus Web site, which shows information about the latest viruses.

## Using the Symantec Network Access Control Home page

If you have Symantec Network Access Control installed, and you have permission to view reports, then your Home page displays automatically generated summaries. These reports contain important information about network compliance status.

Some of the summaries are hyperlinked to more detailed reports. You can click on the chart and the numbers in the summaries to see details.

**Note:** Reports are filtered automatically based on the permissions of the user who is logged on. If you are a system administrator, you see information across domains. If you are a limited administrator with access rights to only one domain, you see information from only that domain.

Figure 9-2 shows how the Symantec Network Access Control Home page appears.

**Figure 9-2** Symantec Network Access Control Home page

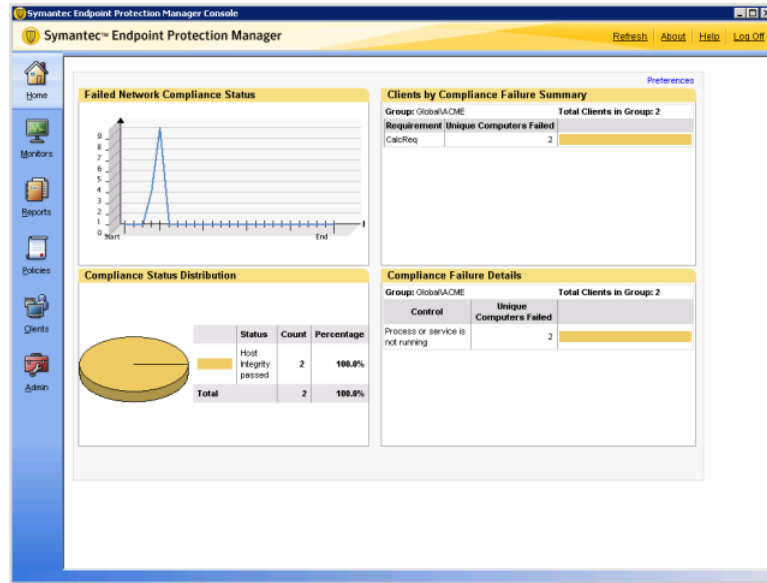


Table 9-5 describes the Home page reports for Symantec Network Access Control.

**Table 9-5** Symantec Network Access Control Home page summaries

Summary	Description
Failed Network Compliance Status	The Failed Network Compliance Status section provides a snapshot of the overall compliance in your network for the configured time period. It displays the clients that tried to connect to the network but cannot because they were out of compliance.

**Table 9-5** Symantec Network Access Control Home page summaries  
*(continued)*

Summary	Description
Compliance Status Distribution	Displays the clients that have failed the Host Integrity check that runs on their computer.
Clients by Compliance Failure Summary	This summary displays the failure rate of the overall compliance requirement. It displays a bar chart that shows a count of the unique workstations by the type of control failure event. Examples of control failure event types are an antivirus, a firewall, or a VPN problem.
Compliance Failure Details	<p>Provides a more detailed bar chart than the Clients by Compliance Failure Summary. For example, suppose the Clients by Compliance Failure Summary shows ten clients with an antivirus compliance failure.</p> <p>In contrast, this report shows the following details:</p> <ul style="list-style-type: none"> <li>■ Four clients have no antivirus software currently in operation on them.</li> <li>■ Two clients have no antivirus software installed.</li> <li>■ Four clients have out-of-date antivirus definitions files.</li> </ul>

If you have only Symantec Network Access Control installed, the Home page reports are not customizable, except for the time period covered by the reports and summaries. You can change the time period by using the Preferences link. The options are the past week and the past 24 hours.

---

**Note:** If you are a system administrator, you see information across domains. If you are a limited administrator with access rights to only one domain, you see information from only that one domain.

---

## Configuring reporting preferences

You can configure the following reporting preferences:

- The Home and Monitors pages display options
- The Security Status thresholds

- The display options that are used for the logs and the reports, as well as legacy log file uploading

For information about the preference options that you can set, you can click **Help** on each tab in the Preferences dialog box.

#### To configure reporting preferences

- 1 From the console, on the Home page, click **Preferences**.
- 2 Click one of the following tabs, depending on the type of preferences that you want to set:
  - **Home and Monitors**
  - **Security Status**
  - **Logs and Reports**
- 3 Set the values for the options that you want to change.
- 4 Click **OK**.

## About Home and Monitors display options

You can set the following preferences for the Home page and the Summary View tab of the Monitors page:

- The unit of time that is used for the reports on the Home page and on the Summary View tab on the Monitors page
- The rate at which the Home page and the Summary View tab on the Monitors page automatically refresh
- The extent of the notifications that are included in the unacknowledged notifications count on the Home page
- The content of the Action Summary on the Home page

By default, you see information for the past 24 hours, but you can change it to the past week if desired.

You can also configure the rate at which the Home page and the Summary View tab on the Monitors page automatically refresh. Valid values range from never to every 5 minutes.

---

**Note:** To configure the rate at which individual logs refresh, you can display the log you want to see. Then, you can select the rate that you want from the Auto-Refresh list box on that log's view.

---

If you are a system administrator, you can configure the Home page count to include only the notifications that you created but have not acknowledged. By default, system administrators see the total number of unacknowledged notifications, regardless of who created the notifications. If you are a limited administrator, the unacknowledged notifications count always consists solely of the notifications that you yourself created but have not acknowledged.

You can configure the Action Summary on the Home page to display by detection count on computers or by the number of computers.

See [“Using the Symantec Endpoint Protection Home page”](#) on page 128.

For descriptions of these display options, see the context-sensitive help for the Home and Monitors tab. You can access the context-sensitive help from the Preferences link on the Home page.

## Configuring security status thresholds

The security status thresholds that you set determine when the Security Status message on the Home page of the management console is considered Poor. Thresholds are expressed as a percentage and reflect when your network is considered to be out of compliance with your security policies. For example, you can set the percentage of computers with out-of-date virus definitions that triggers a poor security status. You can also set how many days old the definitions need to be to qualify as out of date. Symantec Endpoint Protection determines what is current when it calculates whether signatures or definitions are out of date as follows. Its standard is the most current virus definitions and IPS signature dates that are available on the management server on which the management console runs.

---

**Note:** If you have only Symantec Network Access Control installed, you do not have a Security Status tab for configuring security thresholds.

---

For descriptions of these display options, see the context-sensitive help for the Security Status tab. You can access the context-sensitive help from the Preferences link on the Home page.

### To configure security status thresholds

- 1 From the console, on the Home page, click **Preferences**.
- 2 On the Security Status tab, check the items that you want to include in the criteria that determine the overall Home page security status.

- 3 For each item, type the number that you want to trigger a security status of Attention Needed.
- 4 Click **OK**.

## Configuring logs and reports preferences

You can set preferences in the following areas for logs and reports:

- The date format and the date separator that are used for date display
- The number of rows, the time zone, and the IP address format that are used for table display
- The filter display in reports and notifications
- The availability of log data from the computers in the network that run Symantec Antivirus 10.x software

For descriptions of these display options, see the context-sensitive help for the Logs and Reports tab. You can access the context-sensitive help from the Preferences link on the Home page.

---

**Note:** The date display format that you set here does not apply to the virus definitions dates and the versions that display in table columns. These items always use the format Y-M-D.

---

## About the client scan times used in reports and logs

Reports and logs display client scan times using the console's time zone. For example, suppose the client is in the Pacific Time Zone, and it is scanned at 8:00 PM PST. If the console is in the Eastern Time Zone, then the time that is displayed for this scan is 11:00 PM EST.

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 following conditions affect the Set specific dates time filter:

- The accuracy of the data and time on the client
- The accuracy of the data and time on the management server

---

**Note:** If you change the time zone on the server, log off of the console and on again to see accurate times in logs and reports.

---

## About using the Past 24 hours filter in reports and logs

If you select Past 24 hours for the time range of a report or a log view, the range begins when you select the filter. If you refresh the page, the start of the 24-hour range does not reset. If you select the filter and wait to create a report, the time range starts when you selected the filter. This condition also applies when you view an event log or alert log. The time range does not start when you create the report or view the log.

If you want to make sure the past 24-hour range starts now, select a different time range and then reselect Past 24 hours.

---

**Note:** The start of the past 24-hour time range filter on the home page is determined at the time the home page is accessed.

---

## About using the filters that search for groups in reports and logs

Because all groups are subgroups of the Global parent group, when a filter searches for groups, it searches hierarchically starting with the string Global. If the name of the group does not start with the letter g, you should precede the string that you search for with an asterisk. Or, you can begin the string with a g\* when you use wildcard characters.

For example, if you have a group named Services, and you type s\* into this box, no group is found and used in the view. To find a group named Services, you need to use the string \*s\* instead. If you have more than one group that contains the letter s, you may want to use a string such as \*ser\*.





# Viewing and configuring reports

This chapter includes the following topics:

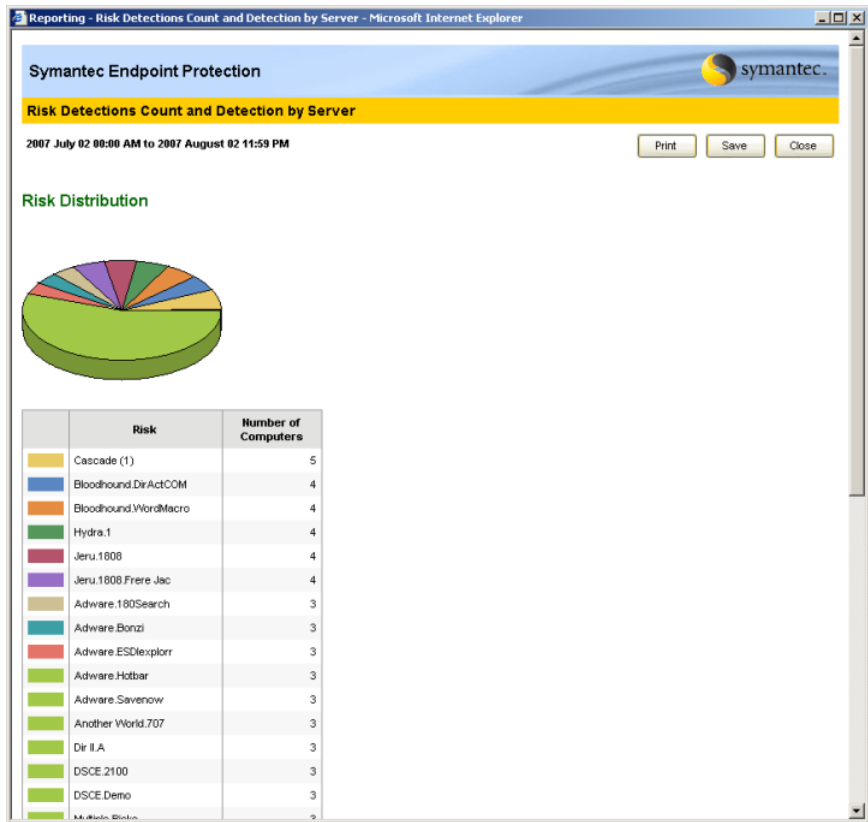
- [Viewing reports](#)
- [About reports](#)
- [Important points about reporting](#)
- [Creating quick reports](#)
- [Saving and deleting saved report filters](#)
- [Printing and saving a copy of a report](#)
- [Creating and deleting scheduled reports](#)

## Viewing reports

Use the Reports page to run, view, print, and schedule reports to run on a regular basis.

[Figure 10-1](#) shows an example of a risk report.

Figure 10-1 Sample report



## About viewing line charts in reports

Line charts show progression over time. The units that are displayed on the x-axis depend on the time range you select.

Table 10-1 shows the x-axis unit that is used for each time range you can select for line charts.

Table 10-1 X-axis units for corresponding time range selected

Time range	X-axis unit
Past 24 Hours	hour

**Table 10-1** X-axis units for corresponding time range selected (*continued*)

Time range	X-axis unit
Past Week	day
Past Month	
Current Month	
Past 3 Months	
Past Year	month
Time range	one day (any 24 hours) is by hour greater than 1 day but less than or equal to 7 days is by hour greater than 7 days but less than or equal to 31 days is by day greater than 31 days but less than or equal to 2 years is by month greater than 2 years is by year

## About viewing bar charts

In the reports that contain histograms or bar charts that involve threats, mouse over the graph bars to see the names of the threats.

## Viewing the reports in Asian languages

Histograms and 3D-bar graphs are created on the server as images before the charts are sent to the browser. By default, the server that you use to create these charts looks for the MS Arial Unicode font. MS Arial Unicode is available as part of Microsoft Office and displays all supported languages correctly. If the MS Arial Unicode font is not found, the server uses the Lucida sans Unicode font.

Some reports on servers that display in an Asian language do not display chart text properly unless MS Arial Unicode is installed on the server. This problem occurs if your report includes a histogram or a 3D-bar graph. If you do not have the MS Arial Unicode font installed on the server, you can configure your server to get around this requirement. You can configure Symantec Endpoint Protection to use any Unicode-enabled font that you have that supports the languages in your environment.

**To change the font used to display reports**

- 1 Change directory to *drive:\Program Files\ Symantec\Symantec Endpoint Protection Manager\Inetpub\Reporting\Common*.
- 2 Open the *i18nCommon.bundle* configuration file with an editor.
- 3 Type the name of the font file that you want to use after the equal sign (=) following the *SPECIAL\_FONT* variable. For example, if you wanted to use Arial, you would type the following:

**SPECIAL\_FONT**=*arial.ttf*

- 4 Save the file in UTF-8 format, and then close the file.
- 5 Make sure that the font file you type is located in the *%WINDIR%\fonts* directory.

## About reports

Quick reports are printable reports available on-demand from the Quick Reports tab on the Reports page.

[Table 10-2](#) describes the report types for quick reports.

**Table 10-2** Quick report types

Report type	Description
Application and Device Control	The Application and Device Control reports contain information about events where access to a computer was blocked or a device was kept off the network.
Audit	The Audit report contains information about policy modification activities, such as the event times and types, policy modifications, domains, sites, administrators, and descriptions.
Compliance	The Compliance reports contain information about the Enforcer server, the Enforcer clients, the Enforcer traffic, and host compliance.
Computer Status	The Computer Status reports contains information about the real-time operational status of the computers in the network.
Network Threat Protection	The Network Threat Protection reports allow you to track a computer’s activity and its interaction with other computers and networks. They record information about the traffic that tries to enter or exit the computers through their network connections.
Risk	The Risk reports include information about risk events on your management servers and their clients.
Scan	The Scan reports provide information about antivirus and antispyware scan activity.

**Table 10-2** Quick report types (*continued*)

Report type	Description
System	The System reports contain information that is useful for troubleshooting client problems.

This section describes the reports by name and their general content. You can configure Basic Settings and Advanced Settings for all reports to refine the data you want to view. You can also save your custom filter with a name to run the same custom report at a later time.

If you have multiple domains in your network, many reports allow you to view data for all domains, one site, or a few sites. The default for all quick reports is to show all domains, groups, servers, and so on, as appropriate for the report you select to create.

---

**Note:** If you have only Symantec Network Access Control installed, a significant number of reports are empty. The Application and Device Control, Network Threat Protection, Risk, and Scan reports do not contain data. The Compliance and Audit reports do contain data, as do some of the Computer Status and System reports.

---

For a description of each configurable option, you can click [Tell me more](#) for that type of report on the console. [Tell me more](#) displays the context-sensitive Help.

See [“Creating quick reports”](#) on page 162.

[Table 10-3](#) describes the Application and Device Control reports that are available.

**Table 10-3** Application and Device Control reports

Report name	Description
Top Groups With Most Alerted Application Control Logs	This report consists of a pie chart with the relative bars. It shows the groups with the application control logs that have generated the largest number of security alerts.
Top Targets Blocked	This report consists of a pie chart with relative bars for each of the following targets, if applicable: <ul style="list-style-type: none"> <li>■ Top Files</li> <li>■ Top Registry Keys</li> <li>■ Top Processes</li> <li>■ Top Modules (dlls)</li> </ul>
Top Devices Blocked	This report consists of a pie chart with a relative bar that shows the devices most frequently blocked from access to your network.

[Table 10-4](#) describes the Audit report that is available.

**Table 10-4**      Audit report

Report name	Description
Policies Used	This report displays the policies that clients and locations use currently. Information includes the domain name, group name, and the serial number of the policy that is applied to each group.

[Table 10-5](#) describes the Compliance reports that are available.

**Table 10-5**      Compliance reports

Report name	Description
Network Compliance Status	<p>This report consists of a line chart and a table. It displays the event time, number of attacks, and the percentage of attacks that are involved in each.</p> <p>You can display the total number of clients to which the following compliance actions have been applied over the time range that you select:</p> <ul style="list-style-type: none"> <li>■ Authenticated</li> <li>■ Disconnected</li> <li>■ Failed</li> <li>■ Passed</li> <li>■ Rejected</li> </ul>
Compliance Status	<p>You can select an action to display a line chart that shows one of the following:</p> <ul style="list-style-type: none"> <li>■ The total number of clients that have passed a host integrity check in your network over the time range that you select</li> <li>■ The total number of clients that have failed a host integrity check in your network over the time range that you select</li> </ul> <p>This report also includes a table that displays the event time, number of clients, and the percentage of clients that are involved in each.</p>
Clients by Compliance Failure Summary	<p>This report consists of a bar chart that shows the following information:</p> <ul style="list-style-type: none"> <li>■ A count of the unique workstations by the type of control failure event, such as antivirus, firewall, or VPN.</li> <li>■ The total number of clients in the group.</li> </ul>
Compliance Failure Details	<p>This report consists of a table that displays the number of unique computers by control failure. It shows the criteria and the rule that is involved in each failure. It includes the percentage of clients that are deployed and the percentage that failed.</p>

**Table 10-5** Compliance reports (*continued*)

Report name	Description
Non-compliant Clients by Location	This report consists of a table that shows the compliance failure events. These events display in groups that are based on their location. Information includes the unique computers that failed, and the percentage of total failures and location failures.

[Table 10-6](#) describes the Computer Status reports that are available.

**Table 10-6** Computer Status reports

Report name	Description
Virus Definitions Distribution	This report displays the unique virus definitions file versions that are used throughout your network and the number of computers and percentage using each version. It consists of a pie chart, a table, and relative bars.
Computers Not Checked into Server	This report displays a list of all the computers that have not checked in with their server. It also displays the computer's IP address, the time of its last checkin, and the user that was logged in at that time.
Symantec Endpoint Protection Product Versions	This report displays the list of version numbers for all the Symantec Endpoint Protection product versions in your network. It also includes the domain and server for each, as well as the number of computers and percentage of each. It consists of a pie chart and relative bars.
Intrusion Prevention Signature Distribution	This report displays the IPS signature file versions that are used throughout your network. It also includes the domain and server for each, as well as the number of computers and percentage of each. It consists of a pie chart and relative bars.
Client Inventory	This report consists of the following charts with relative bars that display the total number of computers and percentage of each: <ul style="list-style-type: none"> <li>■ Operating System</li> <li>■ Total Memory</li> <li>■ Free Memory</li> <li>■ Total Disk Space</li> <li>■ Free Disk Space</li> <li>■ Processor Type</li> </ul>
Compliance Status Distribution	This report consists of a pie chart with relative bars that show compliance passes and failures by group or by subnet. It shows the number of computers and the percentage of computers that are in compliance.

**Table 10-6** Computer Status reports (*continued*)

Report name	Description
Client Online Status	<p>This report consists of pie charts with relative bars per group or per subnet. It displays the percentage of your computers that are online.</p> <p>Online has the following meanings:</p> <ul style="list-style-type: none"> <li>■ For the clients that are in push mode, online means that the clients are currently connected to the server.</li> <li>■ For the clients that are in pull mode, online means that the clients have contacted the server within the last two client heartbeats.</li> <li>■ For the clients in remote sites, online means that the clients were online at the time of the last replication.</li> </ul>
Clients With Latest Policy	<p>This report consists of pie charts with relative bars per group or subnet. It displays the number of computers and percentage that have the latest policy applied.</p>
Client Count by Group	<p>This report consists of a table that lists host information statistics by group. It lists the number of clients and users. If you use multiple domains, this information appears by domain.</p>
Security Status Summary	<p>This report reflects the general security status of the network.</p> <p>This report displays the number and percentage of computers that have the following status:</p> <ul style="list-style-type: none"> <li>■ The Antivirus Engine is off.</li> <li>■ Auto-Protect is off.</li> <li>■ Tamper Protection is off.</li> <li>■ Restart is required.</li> <li>■ A Host Integrity check failed.</li> <li>■ Network Threat Protection is off.</li> </ul>
Protection Content Versions	<p>This report displays all the proactive protection content versions that are used throughout your network in a single report. One pie chart is displayed for each type of protection.</p> <p>The following content types are available:</p> <ul style="list-style-type: none"> <li>■ Decomposer versions</li> <li>■ Eraser Engine versions</li> <li>■ TruScan Proactive Threat Scan Content versions</li> <li>■ TruScan Proactive Threat Scan Engine versions</li> <li>■ Commercial Application List versions</li> <li>■ Proactive Content Handler Engine versions</li> <li>■ Permitted Applications List versions</li> <li>■ The new content types that Symantec Security Response has added</li> </ul>



**Table 10-6** Computer Status reports (*continued*)

Report name	Description
Client Migration	This report consists of tables that describe the migration status of clients by domain, group, and server. It displays the client IP address and whether the migration succeeded, failed, or has not yet started.
Client Software Rollout (Snapshots) This report is available as a scheduled report only.	This report consists of tables that track the progression of client package deployments. The snapshot information lets you see how quickly the rollout progresses, as well as how many clients are still not fully deployed.
Clients Online/Offline Over Time (Snapshots) This report is available as a scheduled report only.	This report consists of line charts and tables that show the number of clients online or offline. One chart displays for each of the top targets. The target is either a group or an operating system.
Clients With Latest Policy over Time (Snapshots) This report is available as a scheduled report only.	This report consists of a line chart that displays the clients that have the latest policy applied. One chart displays for each of the top clients.
Non-compliant Clients Over Time (Snapshots) This report is available as a scheduled report only.	This report consists of a line chart that shows the percentage of clients that have failed a host integrity check over time. One chart displays for each of the top clients.
Virus Definition Rollout (Snapshots) This report is available as a scheduled report only.	This report lists the virus definitions package versions that have been rolled out to clients. This information is useful for tracking the progress of deploying of new virus definitions from the console.

[Table 10-7](#) describes the Network Threat Protection reports that are available.

**Table 10-7** Network Threat Protection reports

Report name	Description
Top Targets Attacked	This report consists of a pie chart with relative bar. You can view information using groups, subnets, clients, or ports as the target. It includes information such as the number and percentage of attacks, the attack type and severity, and the distribution of attacks.

**Table 10-7** Network Threat Protection reports (*continued*)

Report name	Description
Top Sources of Attack	This report consists of a pie chart with relative bars that shows the top hosts that initiated attacks against your network. It includes information such as the number and percentage of attacks, the attack type and severity, and the distribution of attacks.
Top Types of Attack	This report consists of a pie chart with associated relative bars. It includes information such as the number and percentage of events. It also includes the group and severity, as well as the event type and number by group.
Top Blocked Applications	This report consists of a pie chart with relative bars that show the top applications that were prevented from accessing your network. It includes information such as the number and percentage of attacks, the group and severity, and the distribution of attacks by group.
Attacks over Time	This report consists of one or more line charts that display attacks during the selected time period. For example, if the time range is the last month, the report displays the total number of attacks per day for the past month. It includes the number and percentage of attacks. You can view attacks for all computers, or by the top operating systems, users, IP addresses, groups, or attack types.
Security Events by Severity	This report consists of a pie chart that displays the total number and percentage of security events in your network, ranked according to their severity.
Blocked Applications Over Time	This report consists of a line chart and table. It displays the total number of applications that were prevented from accessing your network over a time period that you select. It includes the event time, the number of attacks, and the percentage. You can display the information for all computers, or by group, IP address, operating system, or user.
Traffic Notifications Over Time	This report consists of a line chart. It shows the number of notifications that were based on firewall rule violations over time. The rules that are counted are those where you checked the Send Email Alert option in the Logging column of the Firewall Policy Rules list. You can display the information in this report for all computers, or by group, IP address, operating system, or user.
Top Traffic Notifications	This report consists of a pie chart with relative bars that lists the group or subnet, and the number and percentage of notifications. It shows the number of notifications that were based on firewall rule violations that you configured as important to be notified about. The rules that are counted are those where you checked the Send Email Alert option in the Logging column of the Firewall Policy Rules list. You can view information for all, for the Traffic log, or for the Packet log, grouped by top groups or subnets.

**Table 10-7** Network Threat Protection reports (*continued*)

Report name	Description
Full Report	<p>This report gives you the following Network Threat Protection information in a single report:</p> <ul style="list-style-type: none"> <li>■ Top Types of Attack</li> <li>■ Top Targets Attacked by Group</li> <li>■ Top Targets Attacked by Subnet</li> <li>■ Top Targets Attacked by Client</li> <li>■ Top Sources of Attack</li> <li>■ Top Traffic Notifications by Group (Traffic)</li> <li>■ Top Traffic Notifications by Group (Packets)</li> <li>■ Top Traffic Notifications by Subnet (Traffic)</li> <li>■ Top Traffic Notifications by Subnet (Packets)</li> </ul> <p>This report includes the information for all domains.</p>

[Table 10-8](#) describes the Risk reports that are available.

**Table 10-8** Risk reports

Report name	Description
Infected and At Risk Computers	This report consists of two tables. One table lists computers that have a virus infection. The other table lists the computers that have a security risk that has not yet been remediated.
Detection Action Summary	This report consists of a table that shows a count of all the possible actions that were taken when risks were detected. The possible actions are Cleaned, Suspicious, Blocked, Quarantined, Deleted, Newly Infected, and Still Infected. This information also appears on the Symantec Endpoint Protection Home page.
Risk Detections Count	This report consists of a pie chart, a risk table, and an associated relative bar. It shows the total number of risk detections by domain, server, or computer. If you have legacy Symantec AntiVirus clients, the report uses the server group rather than the domain.

**Table 10-8** Risk reports (*continued*)

Report name	Description
<p>New Risks Detected in the Network</p>	<p>This report includes a table and a distribution pie chart.</p> <p>For each new risk, the table provides the following information:</p> <ul style="list-style-type: none"> <li>■ Risk name</li> <li>■ Risk category or type</li> <li>■ First discovered date</li> <li>■ First occurrence in the organization</li> <li>■ Scan type that first detected it</li> <li>■ Domain where it was discovered (server group on legacy computers)</li> <li>■ Server where it was discovered (parent server on legacy computers)</li> <li>■ Group where it was discovered (parent server on legacy computers)</li> <li>■ The computer where it was discovered and the name of the user that was logged on at the time</li> </ul> <p>The pie chart shows new risk distribution by the target selection type: domain (server group on legacy computers), group, server (parent server on legacy computers), computer, or user name.</p>
<p>Top Risk Detections Correlation</p>	<p>This report consists of a three-dimensional bar graph that correlates virus and security risk detections by using two variables. You can select from computer, user name, domain, group, server, or risk name for the x and y axis variables. This report shows the top five instances for each axis variable. If you selected computer as one of the variables and there are fewer than five infected computers, non-infected computers may appear in the graph.</p> <p><b>Note:</b> For computers running legacy versions of Symantec AntiVirus, the server group and parent server are used instead of domain and server.</p>
<p>Risk Distribution Summary</p>	<p>This report includes a pie chart and an associated bar graph that displays a relative percentage for each unique item from the chosen target type. For example, if the chosen target is risk name, the pie chart displays slices for each unique risk. A bar is shown for each risk name and the details include the number of detections and its percentage of the total detections. Targets include the risk name, domain, group, server, computer, user name, source, risk type, or risk severity. For computers running legacy versions of Symantec AntiVirus, the server group and parent server are used instead of domain and server.</p>
<p>Risk Distribution Over Time</p>	<p>This report consists of a table that displays the number of virus and security risk detections per unit of time and a relative bar.</p>

**Table 10-8** Risk reports (*continued*)

Report name	Description
TruScan Proactive Threat Scan Detection Results	<p>This report consists of a pie chart and bar graphs that display the following information:</p> <ul style="list-style-type: none"> <li>■ A list of the applications that are labeled as risks that you have added to your exceptions as acceptable in your network.</li> <li>■ A list of the applications that have been detected that are confirmed risks.</li> <li>■ A list of the applications that have been detected but whose status as a risk is still unconfirmed.</li> </ul> <p>For each list, this report displays the company name, the application hash and the version, and the computer involved. For the permitted applications, it also displays the source of the permission.</p>
TruScan Proactive Threat Distribution	<p>This report consists of a pie chart that displays the top application names that have been detected with relative bars and a summary table. The detections include applications on the Commercial Applications List and Forced Detections lists. The first summary table contains the application name and the number and percentage of detections.</p> <p>The summary table displays the following, per detection:</p> <ul style="list-style-type: none"> <li>■ Application name and hash</li> <li>■ Application type, either keylogger, Trojan horse, worm, remote control, or commercial keylogger</li> <li>■ Company name</li> <li>■ Application version</li> <li>■ Number of unique computers that have reported the detection</li> <li>■ Top three path names in the detections</li> <li>■ Date of last detection</li> </ul>
TruScan Proactive Threat Detection over Time	<p>This report consists of a line chart that displays the number of proactive threat detections for the time period selected. It also contains a table with relative bars that lists the total numbers of the threats that were detected over time.</p>
Action Summary for Top Risks	<p>This report lists the top risks that have been found in your network. For each, it displays action summary bars that show the percentage of each action that was taken when a risk was detected. Actions include quarantined, cleaned, deleted, and so on. This report also shows the percentage of time that each particular action was the first configured action, the second configured action, neither, or unknown.</p>
Number of Notifications	<p>This report consists of a pie chart with an associated relative bar. The charts show the number of notifications that were triggered by the firewall rule violations that you have configured as important to be notified about. It includes the type of notifications and the number of each.</p> <p>See <a href="#">“Configuring email messages for traffic events”</a> on page 476.</p>

**Table 10-8** Risk reports (*continued*)

Report name	Description
Number of Notifications over Time	This report consists of a line chart that displays the number of notifications in the network for the time period selected. It also contains a table that lists the number of notifications and percentage over time. You can filter the data to display by the type of notification, acknowledgment status, creator, and notification name.
Weekly Outbreaks	This report displays the number of virus and security risk detections and a relative bar per week for each for the specified time range. A range of one day displays the past week.
Comprehensive Risk Report	By default, this report includes all of the distribution reports and the new risks report. However, you can configure it to include only certain of the reports. This report includes the information for all domains.

[Table 10-9](#) describes the Scan reports that are available.

**Table 10-9** Scan reports

Report name	Description
Scan Statistics Histogram	<p>This report is presented as a histogram. You can select how you want the information in the scan report to be distributed. You can select one of the following methods:</p> <ul style="list-style-type: none"> <li>■ By the scan time (in seconds)</li> <li>■ By the number of risks detected</li> <li>■ By the number of files with detections</li> <li>■ By the number of files that are scanned</li> <li>■ By the number of files that are omitted from scans</li> </ul> <p>You can also configure the bin width and how many bins are used in the histogram. The bin width is the data interval that is used for the group by selection. The number of bins specifies how many times the data interval is repeated in the histogram.</p> <p>The information that displays includes the number of entries and the minimum and the maximum values, as well as the average and the standard deviation.</p> <p>You might want to change the report values to maximize the information that is generated in the report's histogram. For example, you might want to consider the size of your network and the amount of information that you view.</p>
Computers by Last Scan Time	This report shows a list of computers in your security network by the last time scanned. It also includes the IP address and the name of the user that was logged in at the time of the scan.

**Table 10-9** Scan reports (*continued*)

Report name	Description
Computers Not Scanned	<p>This report shows a list of computers in your security network that have not been scanned.</p> <p>This report provides the following additional information:</p> <ul style="list-style-type: none"> <li>■ The IP address</li> <li>■ The time of the last scan</li> <li>■ The name of the current user or the user that was logged on at the time of the last scan</li> </ul>

[Table 10-10](#) describes the System reports that are available.

**Table 10-10** System reports

Report name	Description
Top Clients That Generate Errors	This report consists of a pie chart for each warning condition and error condition. The charts show the relative error count and relative warning count and percentage, by client.
Top Servers That Generate Errors	This report consists of a pie chart for each warning condition and error condition. The charts show the relative error count and relative warning count and percentage, by server.
Top Enforcers That Generate Errors	This report consists of a pie chart for each warning condition and error condition. The charts show the relative error count and relative warning count and percentage, by Enforcer.
Database Replication Failures Over Time	This report consists of a line chart with an associated table that lists the replication failures for the time range selected.

**Table 10-10** System reports (*continued*)

Report name	Description
Site Status	<p>This report displays the current status and throughput of all servers in your local site. It also shows information about client installation, client online status, and client log volume for your local site. The data this report draws from is updated every ten seconds, but you need to rerun the report to see updated data.</p> <p><b>Note:</b> If you have multiple sites, this report shows the total installed and online clients for your local site, not all your sites.</p> <p>If you have site or domain restrictions as an administrator, you only see the information that you are allowed to see.</p> <p>The health status of a server is classified as follows:</p> <ul style="list-style-type: none"> <li>■ Good: The server is up and works normally</li> <li>■ Poor: The server is low on memory or disk space, or has a large number of client request failures.</li> <li>■ Critical: The server is down</li> </ul> <p>For each server, this report contains the status, health status and reason, CPU and memory usage, and free disk space. It also contains server throughput information, such as policies downloaded, and site throughput sampled from the last heartbeat.</p> <p>It includes the following site throughput information:</p> <ul style="list-style-type: none"> <li>■ Total clients installed and online</li> <li>■ Policies downloaded per second</li> <li>■ Intrusion Prevention signatures downloaded per second</li> <li>■ Learned applications per second</li> <li>■ Client Logs received per second</li> <li>■ Policies downloaded per second</li> <li>■ Intrusion Prevention System signatures downloaded per second</li> <li>■ Learned applications per second</li> <li>■ Enforcer system logs, traffic logs, and packet logs per second</li> <li>■ Client information updates per second</li> <li>■ Client security logs, system logs, traffic logs, and packet logs received per second</li> <li>■ Application and device control logs received per second</li> </ul> <p>Online has the following meanings in this report:</p> <ul style="list-style-type: none"> <li>■ For the clients that are in push mode, online means that the clients are currently connected to the server.</li> <li>■ For the clients that are in pull mode, online means that the clients have contacted the server within the last two client heartbeats.</li> <li>■ For the clients in remote sites, online means that the clients were online at the time of the last replication.</li> </ul>



# Important points about reporting

You should be aware of the following information when you use reports:

- Timestamps in reports 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.
- 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.
- Risk category information in the reports is obtained from the Symantec Security Response Web site. Until the console is able to retrieve this information, any reports that you generate show Unknown in the risk category fields.
- The reports that you generate give an accurate picture of compromised computers in your network. Reports are based on log data, not the Windows registry data.
- Report pages and log pages always display in the language that the management server was installed with. To display these pages when you use a remote console or browser, you must have the appropriate font installed on the computer that you use.
- If you get database errors when you run a report that includes a large amount of data, you might want to change database timeout parameters. See "[Changing timeout parameters](#)" on page 284.
- If you get CGI or terminated process errors, you might want to change other timeout parameters. See the Symantec Knowledge Base article "Reporting server does not report or shows a timeout error message when you query large amounts of data."

The following information is important to note if you have computers in your network that are running legacy versions of Symantec AntiVirus:

- When you use report and log filters, server groups are categorized as domains. Client groups are categorized as groups, and parent servers are categorized as servers.
- If you generate a report that includes legacy computers, the IP address and MAC address fields display None.

# Creating quick reports

Generate a quick report by selecting from the Basic Settings options that appear under "What filter settings would you like to use." If you want to configure additional options to construct a report, click Advanced Settings. The Basic Settings and Advanced Settings vary from report to report.

For a description of each advanced setting that you can configure, you can click Tell me more for that type of report on the console. Clicking Tell me more displays the context-sensitive Help for that type of report.

You can save the report settings so that you can run the same report at a later date, and you can print and save reports.

---

**Note:** The filter option text boxes that accept wildcard characters and search for matches are not case-sensitive. The ASCII asterisk character is the only asterisk character that can be used as a wildcard character.

---

See ["Printing and saving a copy of a report"](#) on page 167.

[Table 10-11](#) describes all the Basic Settings available for all types of quick report.

**Table 10-11** Basic filter settings for quick reports

Setting	Description
Time range	<p>Specifies the time range of events you want to view in the report.</p> <p>Select from the following times:</p> <ul style="list-style-type: none"> <li>■ Past 24 hours</li> <li>■ Past week</li> <li>■ Past month</li> <li>■ Current month</li> <li>■ Past three months</li> <li>■ Past year</li> <li>■ Set specific dates</li> </ul> <p>If you choose Set specific dates, some reports require that you set a Start date and End date. Other reports require that you set the Last checkin time, which is the last time that the computer checked in with its server.</p> <p>The default is Past 24 hours.</p>
Start date	<p>Specifies the start date for the date range.</p> <p>Only available when you select Set specific dates for the time range.</p>

**Table 10-11** Basic filter settings for quick reports (*continued*)

Setting	Description
End date	<p>Specifies the end date for the date range.</p> <p>Only available when you select Set specific dates for the time range.</p> <p><b>Note:</b> You cannot set an end date that is the same as the start date or earlier than the start date.</p>
Last checkin after	<p>Specifies that you want to see all entries that involve a computer that has not checked in with its server since this time.</p> <p>Only available for Computer Status reports when you select Set specific dates for the time range.</p>
Status	<p>Available for the Network Compliance Status Compliance report. Select from the following:</p> <ul style="list-style-type: none"><li>■ Authenticated</li><li>■ Disconnected</li><li>■ Failed</li><li>■ Passed</li><li>■ Rejected</li></ul> <p>Available for the Compliance Status Compliance report. Select from the following actions:</p> <ul style="list-style-type: none"><li>■ Passed</li><li>■ Failed</li></ul>
Group By	<p>Many of the reports can be grouped in appropriate ways. For example, the most common choice is to view information for only one group or subnet, but some reports provide other appropriate choices.</p>

**Table 10-11** Basic filter settings for quick reports (*continued*)

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

**Table 10-11** Basic filter settings for quick reports (*continued*)

Setting	Description
Number of bins	Specifies the number of bins you want used to form the bars of a histogram. Available for the Scan Statistics Histogram Scan report.

The Advanced Settings provide additional control over the data that you want to view. They are specific to the report type and content.

For a description of each advanced setting that you can configure, you can click **Tell me more** for that type of report on the console. Clicking **Tell me more** displays the context-sensitive Help for that type of report.

#### To create a quick report

- 1 In the console, click **Reports**.
- 2 On the Quick Reports tab, in the Report type list box, select the type of report that you want to create. For example, select **Risk**.
- 3 Under **What type of Scan Report would you like to see**, in the Select a report list box, select the name of the report you want to view. For example, select **Risk Detections Count**.
- 4 In the Use saved filter list box, select a saved filter configuration that you want to use, or leave the default filter.
- 5 Under **What filter settings would you like to use**, in the Time range list box, select the time range for the report.
- 6 If you selected **Set specific dates**, then use the Start date and End date list boxes. These options set the time interval that you want to view information about.
- 7 If you want to configure additional settings for the report, click **Advanced Settings** and set the options that you want. You can click **Tell me more** on the Quick Reports tab to see descriptions of the filter options in the context-sensitive Help.

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

You can save the report configuration settings if you think you will want to run this report again in the future.

See [“Saving and deleting saved report filters”](#) on page 166.

- 8 Click **Create Report**.

## Saving and deleting saved report filters

You can save custom report settings so that you can generate the report again at a later date. When you save your settings, they are saved in the database. The name you give to the filter appears in the Use a saved filter list box for that type of logs and reports.

---

**Note:** The filter configuration settings that you save are available for your user logon account only. Other users with reporting privileges do not have access to your saved settings.

---

You can delete any report configuration that you create. When you delete a configuration, the report is no longer available. The default report configuration name appears in the Use a saved report list box and the screen is repopulated with the default configuration settings.

### To save a filter

- 1 In the console, click **Reports**.
- 2 Select a report type from the list box.
- 3 Change any Basic Settings or Advanced Settings for the report.
- 4 Click **Save Filter**.
- 5 In the Filter name text box, type a descriptive name for this report filter. Only the first 32 characters of the name that you give display when the filter is added to the Use a saved filter list.
- 6 Click **OK**.
- 7 When the confirmation dialog box appears, click **OK**.

After you save a filter, it appears in the Use a saved filter list box for related reports and logs.

### To delete a saved filter

- 1 On the Reports tab, select a report type.
- 2 In the Use saved filter list box, select the name of the filter that you want to delete.
- 3 Click the Delete icon beside the Use a saved filter list box.
- 4 When the confirmation dialog box appears, click **Yes**.

## About duplicate filter names

Filter storage is based in part on the creator, so problems do not occur when two different users create a filter with the same name. However, a single user or two users who log on to the default admin account should not create filters with the same name.

If users create filters with the same name, a conflict can occur under two conditions:

- Two users are logged on to the default admin account on different sites and each creates a filter with the same name.
- One user creates a filter, logs on to a different site, and immediately creates a filter with the same name.

If either condition occurs before site replication takes place, the user subsequently sees two filters with the same name in the filter list. Only one of the filters is usable. If this problem occurs, it is a best practice to delete the usable filter and recreate it with a different name. When you delete the usable filter, you also delete the unusable filter.

## Printing and saving a copy of a report

When you generate a report, the report appears in a new window. You can print the report or save a copy of the report.

---

**Note:** By default, Internet Explorer does not print background colors and images. If this printing option is disabled, the printed report may look different than the report that you created. You can change the settings in your browser to print background colors and images.

---

### To print a copy of a report

- 1 In the report window, click **Print**.
- 2 In the Print dialog box, select the printer you want, if necessary, and then click **Print**.

When you save a report, you save a snapshot of your security environment that is based on the current data in your reporting database. If you run the same report later, based on the same filter configuration, the new report shows different data.

### To save a copy of a report

- 1 In the report window, click **Save**.
- 2 In the File Download dialog box, click **Save**.

- 3 In the Save As dialog box, in the Save in selection box, browse to the location where you want to save the file.
- 4 In the File name list box, change the default file name, if desired.
- 5 Click **Save**.  
The report is saved in Microsoft Web Archive format, single file (\*.mht) in the location you selected.
- 6 In the Download complete dialog box, click **Close**.

## Creating and deleting 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 snapshot reports is updated in the database every hour. Scheduled reports are emailed to their recipients at the hour and time that the administrator configures by using the Run every option. At the time that Symantec Endpoint Protection emails a snapshot report, the data in the report is current to within one hour. The other reports that contain data over time are updated in the database based on the upload interval that you configured for the client logs.

See [“Configuring client log settings”](#) on page 279.

---

**Note:** If you have multiple servers within a site that share a database, only the first-installed server runs the reports scheduled for the site. This default ensures that all the servers in the site do not run the same scheduled scans simultaneously. If you want to designate a different server to run scheduled reports, you can configure this option in the local site properties.

See [“Editing site properties”](#) on page 226.

---

The following quick reports are only available as scheduled reports:

- Client Software Rollout (Snapshots)
- Clients Online/Offline Over Time (Snapshots)
- Clients With Latest Policy over Time (Snapshots)
- Non-Compliant Clients Over Time (Snapshots)
- Virus Definition Rollout (Snapshots)



You can change the settings for any report that you have already scheduled. The next time the report runs it uses the new filter settings. You can also create additional scheduled reports, which you can associate with a previously saved report filter. You can delete a single scheduled report or all of the scheduled reports.

---

**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.

---

You can print and save scheduled reports, as you do with the reports that you run on-demand.

---

**Note:** When you first create a scheduled report, you must use the default filter or a filter you've already saved. After you have scheduled the report, you can go back and edit the filter.

---

For information about the options you can set in these procedures, on the Scheduled Reports tab, you can click [Tell me more](#).

#### To create a scheduled report

- 1 In the console, click **Reports**.
- 2 On the Scheduled Reports tab, click **Add**.
- 3 In the Report name text box, type a descriptive name and optionally, type a longer description.  
Although you can paste more than 255 characters into the description text box, only 255 characters are saved in the description.
- 4 Uncheck the **Enable this scheduled report** check box if you do not currently want this report to run.
- 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 (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 Under Report Schedule, in the Run every text box, type the frequency with which this report should be emailed to recipients.
- 10 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.
- 11 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.
- 12 Click **OK** to save the scheduled report configuration.

**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**.

**To delete a scheduled report**

- 1 In the console, click **Reports**.
- 2 On the Scheduled Reports tab, in the list of reports, click the name of the report that you want to delete.
- 3 Click **Delete**.
- 4 When the confirmation dialog box appears, click **Yes**.

# Viewing and configuring logs and notifications

This chapter includes the following topics:

- [About logs](#)
- [Using the Monitors Summary tab](#)
- [Viewing logs](#)
- [Saving and deleting filters](#)
- [Basic filter settings for logs](#)
- [Advanced filter settings for logs](#)
- [Running commands and actions from logs](#)
- [About reducing the volume of events sent to the logs](#)
- [Exporting log data](#)
- [Using notifications](#)

## About logs

Using the logs, you can view detailed events from your security products. Logs contain event data from your management servers as well as all the clients that communicate with those servers. Because reports are static and do not include as much detail as the logs, some administrators prefer to monitor their network primarily by using logs.

You may want to view this information to troubleshoot security or connectivity problems in your network. This information may also be useful for the investigation of threats or to verify the history of events.

---

**Note:** Report pages and log pages always display in the language that the management server was installed with. To display these pages when you use a remote console or browser, you must have the appropriate font installed on the computer that you use.

---

You can export some log event data to a comma-delimited file for importing into a spreadsheet application. Other log data can be exported to a dump file or a Syslog server.

See [“Exporting log data”](#) on page 189.

## About log types, contents, and commands

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

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

---

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

---

Some types of logs are further divided into different types of content to make easier to view. For example, Application Control and Device Control logs include the Application Control log and the Device Control log. You can also run commands from some logs.

See [“Viewing and filtering administrator notification information”](#) on page 193.

**Note:** If you have only Symantec Network Access Control installed, only some of the logs contain data; some logs are empty. The Audit log, Compliance log, Computer Status log, and System log contain data. If you have only Symantec Endpoint Protection installed, the Compliance logs and Enforcer logs are empty but all other logs contain data.

Table 11-1 describes the different types of content that you can view and the actions that you can take from each log.

**Table 11-1** Log and lists

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

**Table 11-1** Log and lists (*continued*)

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

**Table 11-1** Log and lists (*continued*)

Log type	Contents and actions
Computer Status	<p>The Computer Status log contains information about the real-time operational status of the client computers in the network. Information available includes the computer name and IP address, last checkin time, definitions date, infected status, Auto-Protect status, server, group, domain, and user name.</p> <p>You can perform the following actions from the Computer Status log:</p> <ul style="list-style-type: none"> <li>■ <b>Scan</b> This command launches an Active, Full, or Custom scan. Custom scan options are those that you have set for command scans on the Administrator-defined Scan page. The command uses the settings in the Antivirus and Antispyware Policy that applies to the clients that you selected to scan.</li> <li>■ <b>Update Content</b> This command triggers an update of policies, definitions, and software from the console to the clients in the selected group.</li> <li>■ <b>Update Content and Scan</b> This command triggers an update of the policies, definitions, and software on the clients in the selected group. This command then launches a Active, Full, or Custom scan. Custom scan options are those that you have set for command scans on the Administrator-defined Scan page. The command uses the settings in the Antivirus and Antispyware Policy that applies to the clients that you selected to scan.</li> <li>■ <b>Cancel All Scans</b> This command cancels all running scans and any queued scans on the selected recipients.</li> <li>■ <b>Restart Computers</b> This command restarts the computers that you selected. If users are logged on, they are warned about the restart based on the restart options that the administrator configured for that computer. You can configure client restart options on the General Settings tab of the General Settings dialog boulder Settings on the Clients page.</li> <li>■ <b>Enable Auto-Protect</b> This command turns Auto-Protect on for all the client computers that you selected.</li> <li>■ <b>Enable Network Threat Protection</b> This command turns on Network Threat Protection for all the client computers that you selected.</li> <li>■ <b>Disable Network Threat Protection</b> This command turns Network Threat Protection off for all the client computers that you selected.</li> </ul> <p>You can also clear the infected status of computers from this log.</p>

**Table 11-1** Log and lists (*continued*)

Log type	Contents and actions
Network Threat Protection	<p>The Network Threat Protection logs contain information about attacks on the firewall and on intrusion prevention. Information is available about denial-of-service attacks, port scans, and the changes that were made to executable files. They also contain information about the connections that are made through the firewall (traffic), and the data packets that pass through. These logs also contains some of the operational changes that are made to computers, such as detecting network applications, and configuring software. Information available includes items such as the time, the event type; and the action taken. Additional information available includes the severity; the direction, the host name, the action taken, the IP address, and the protocol involved.</p> <p>The following Network Threat Protection logs are available:</p> <ul style="list-style-type: none"> <li>■ Attacks</li> <li>■ Traffic</li> <li>■ Packet</li> </ul> <p>No actions are associated with these logs.</p>
TruScan Proactive Threat Scan	<p>The TruScan Proactive Threat Scan log contains information about the threats that have been detected during proactive threat scanning. TruScan proactive threat scans use heuristics to scan for any behavior that is similar to virus and security risk behavior. This method can detect unknown viruses and security risks. Available information includes items such as the time of occurrence, event name, computer and user involved, the application name and type, and the file name.</p> <p>You can add a detected process to a preexisting Centralized Exceptions Policy from this log.</p>
Risk	<p>The Risk log contains information about risk events. Some of the information available includes the event name and time, user name, computer, risk name, count, source, and path name.</p> <p>You can take the following actions from this log:</p> <ul style="list-style-type: none"> <li>■ Add Risk to Centralized Exceptions Policy</li> <li>■ Add File to Centralized Exceptions Policy</li> <li>■ Add Folder to Centralized Exceptions Policy</li> <li>■ Add Extension to Centralized Exceptions Policy</li> <li>■ Delete from Quarantine</li> </ul>
Scan	<p>The Scan log contains information about antivirus and antispysware scan activity. Information available includes items such as the computer name, IP address, status, scan time, duration, and scan results.</p> <p>No actions are associated with these logs.</p>



**Table 11-1** Log and lists (*continued*)

Log type	Contents and actions
System	<p>The system logs contain information about events such as when services start and stop. Information available includes items such as event time and event type; the site, domain, and server involved; and severity.</p> <p>The following system logs are available:</p> <ul style="list-style-type: none"> <li>■ Administrative</li> <li>■ Client-Server Activity</li> <li>■ Server Activity</li> <li>■ Client Activity</li> <li>■ Enforcer Activity</li> </ul> <p>No actions are associated with these logs.</p>
Command Status list	<p>The Command Status list contains information about the status of commands that you have run from the console. It includes information such as the date the command was run, who issued it, and a description of the command. It also includes the completion status of the command and the clients that the command affected.</p>
Notifications list	<p>The Notifications list contains information about notification events. Such events include information such as the date and time of the notification. It also includes whether or not the notification was acknowledged, who created it, its subject, and the message.</p> <p>No actions are associated with these logs.</p> <p><b>Note:</b> The Notifications log is accessed from the Notifications tab on the Monitors page, not from the Logs tab.</p> <p>See <a href="#">“Viewing and filtering administrator notification information”</a> on page 193.</p>

## Using the Monitors Summary tab

The Summary tab on the Monitors tab displays concise, high-level summaries of important log data to give you an immediate picture of security status.

You can view the following summaries on the Summary tab:

- Antivirus and Antispyware Protection
- Network Threat Protection
- Compliance
- Site Status

[Table 11-2](#) lists the contents of the summary views.

**Table 11-2** Summary views and their contents

Summary view	Contents
Antivirus	<p>The Antivirus view contains the following information:</p> <ul style="list-style-type: none"> <li>■ TruScan Proactive Threats</li> <li>■ Risk Distribution</li> <li>■ New Risks</li> <li>■ Risk Distribution by Source</li> <li>■ Risk Distribution by Attacker</li> <li>■ Risk Distribution by Group</li> </ul> <p><b>Note:</b> New Risks are calculated from the last database sweep and for the time period that is configured on the Home and Monitors tab of Preferences.</p> <p>See <a href="#">“About Home and Monitors display options”</a> on page 140.</p> <p>For example, suppose your Preferences time range is set to the default value, the past 24 hours. And suppose that your database is set to sweep every week on Sunday night and delete the risks that are more than three days old. If a particular virus infects a computer in your network on Monday, that is reported as a new risk. If another computer is infected with the same virus on Wednesday, that is not reflected in this count. If this same virus infects a computer in your network on the following Monday, it is reported here as newly infected. It is reported as new because it occurred during the last 24 hours and Sunday the database was swept of entries older than three days. The previous risk detections occurred more than three days ago, so they were deleted from the database.</p>
Network Threat Protection	<p>The Network Threat Protection view contains the following information:</p> <ul style="list-style-type: none"> <li>■ Top Targets Attacked by Group</li> <li>■ Attack Event Types</li> <li>■ Top Sources of Attack</li> <li>■ Security Events by Severity</li> </ul>

**Table 11-2** Summary views and their contents (*continued*)

Summary view	Contents
Compliance	<p>The Compliance view contains the following information:</p> <ul style="list-style-type: none"><li>■ Failed Network Compliance Status</li><li>■ Compliance Status Distribution</li><li>■ Clients by Compliance Failure Summary</li><li>■ Compliance Failure Details</li></ul> <p><b>Note:</b> If you do not have Symantec Network Access Control installed, the Compliance view contains no data.</p>
Site Status	<p>The Site Status view contains the following information:</p> <ul style="list-style-type: none"><li>■ Site Status</li><li>■ Top Error Generators By Server</li><li>■ Top Error Generators By Client</li><li>■ Replication Failures Over Time</li><li>■ Top Error Generators By Enforcer</li></ul> <p><b>Note:</b> If you do not have Symantec Network Access Control installed, Top Error Generators By Enforcer contains no data.</p>

If you have only Symantec Network Access Control installed, you should note the following information:

- The Compliance view that is described in [Table 11-2](#) comprises your Home page.
- Site Status is the only view available on your Summary tab.

You can click any of the pie charts in the Summary tab view to see more details. For the Top Targets Attacked by summary under Network Threat Protection, use the list box to see the summary by groups, subnets, clients, or ports.

---

**Note:** If you have only Symantec Endpoint Protection installed, the charts in the Compliance summary view are empty. If you have only Symantec Network Access Control installed, the Summary tab contains only the Site Status view. You can view the Compliance summary information on the Home page.

---

### To change the summary type

- 1 In the main window, click **Monitors**.
- 2 At the top of the Summary tab, in the Summary type list box, select the type of view that you want to see.

## Viewing logs

You can generate a list of events to view from your logs that are based on a collection of filter settings that you select. Each log type and content type has a default filter configuration that you can use as-is or modify. You can also create and save new filter configurations. These new filters can be based on the default filter or on an existing filter that you created previously. If you save the filter configuration, you can generate the same log view at a later date without having to configure the settings each time. You can delete your customized filter configurations if you no longer need them.

See [“Saving and deleting filters”](#) on page 182.

---

**Note:** If database errors occur when you view the logs that include a large amount of data, you might want to change the database timeout parameters.

See [“Changing timeout parameters”](#) on page 284.

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

For information about additional timeout parameters, see the Symantec Knowledge Base article "Reporting server does not report or shows a timeout error message when querying large amounts of data."

---

Because logs contain some information that is collected at intervals, you can refresh your log views. To configure the log refresh rate, display the log and select from the Auto-Refresh list box at the top right on that log's view.

---

**Note:** If you view log data by using specific dates, Auto-Refresh has no effect. The data always stay the same.

---

For a description of each configurable option, you can click Tell me more for that type of report on the console. Tell me more displays the context-sensitive Help.

---

**Note:** The filter option fields that accept wildcard characters and search for matches are not case-sensitive. The ASCII asterisk character is the only asterisk character that can be used as a wildcard character.

---

#### To view a log

- 1 In the main window, click **Monitors**.
- 2 On the Logs tab, from the Log type list box, select the type of log that you want to view.
- 3 For some types of logs, a Log content list box appears. If it appears, select the log content that you want to view.
- 4 In the Use a saved filter list box, select a saved filter or leave the value Default.
- 5 Select a time from the Time range list box or leave the default value. If you select **Set specific dates**, then set the date or dates and time from which you want to display entries.
- 6 Click **Advanced Settings** to limit the number of entries you display. You can also set any other available **Advanced Settings** for the type of log that you selected.
- 7 After you have the view configuration that you want, click **View Log**.  
The log view appears in the same window.

## Displaying event details in logs

You can display details about the events that are stored in the logs.

#### To display event details

- 1 In the main window, click **Monitors**.
- 2 On the Logs tab, from the Log type list box, select the type of log that you want to view.
- 3 For some types of logs, a Log content list box appears. If it appears, select the log content that you want to view.
- 4 Click **View Log**.
- 5 Click the event that you want to view the details of, and then click **Details**.

## Viewing logs from other sites

If you want to view the logs from another site, you must log in to a server at the remote site from the console. If you have an account on a server at the remote site, you can log on remotely and view that site's logs.

If you have configured replication partners, you can choose to have all the logs from the replication partners copied to the local partner and vice versa.

See [“Replicating logs”](#) on page 296.

If you choose to replicate logs, by default you see the information from both your site and the replicated sites when you view any log. If you want to see a single site, you must filter the data to limit it to the location you want to view.

---

**Note:** If you choose to replicate logs, be sure that you have sufficient disk space for the additional logs on all the replication partners.

---

#### To view the logs from another site

- 1 Open a Web browser.
- 2 Type the server name or IP address and the port number, 9090, in the address text box as follows:

**http://192.168.1.100:9090**

The console then downloads. The computer from which you log on must have the Java 2 Runtime Environment (JRE) installed. If it does not, you are prompted to download and install it. Follow the prompts to install the JRE.

See [“Logging on to the Symantec Endpoint Protection Manager”](#) on page 29.

- 3 In the console logon dialog box, type your user name and password.
- 4 In the Server text box, if it does not fill automatically, type the server name or IP address and port number 8443 as follows:

**http://192.168.1.100:8443**

- 5 Click **Log On**.

## Saving and deleting filters

You can construct custom filters by using the Basic Settings and Advanced Settings to change the information that you want to see. You can save your filter settings to the database so that you can generate the same view again in the future. When you save your settings, they are saved in the database. The name you give to the filter appears in the Use a saved filter list box for that type of logs and reports.

---

**Note:** If you selected Past 24 hours as the time range for a log filter, the 24-hour time range begins when you first select the filter. If you refresh the page, the start of the 24-hour range does not reset. If you select the filter, and wait to view a log, the time range starts when you select the filter. It does not start when you view the log.

If you want to make sure the past 24-hour range starts now, select a different time range and then reselect Past 24 hours.

---

#### To save a filter

- 1 In the main window, click **Monitors**.
- 2 On the Logs tab, select the type of log view that you want to configure a filter for from the Log type list box.
- 3 For some types of logs, a Log content list box appears. If it appears, select the log content that you want to configure a filter for.
- 4 In the Use a saved filter list box, select the filter that you want to start from. For example, select the default filter.
- 5 Under What filter settings would you like to use, click **Advanced Settings**.
- 6 Change any of the settings.
- 7 Click **Save Filter**.
- 8 In the dialog box that appears, in the Filter name box, type the name that you want to use for this log filter configuration. Only the first 32 characters of the name that you give display when the saved filter is added to the filter list.
- 9 Click **OK** and your new filter name is added to the Use a saved filter list box.
- 10 When the confirmation dialog box appears, click **OK**.

#### To delete a saved filter

- 1 In the Use a saved filter list box, select the name of the log filter that you want to delete.
- 2 Beside the Use a saved filter list box, click the **Delete** icon.
- 3 When you are prompted to confirm that you want to delete the filter, click **Yes**.

## About duplicate filter names

Filter storage is based in part on the creator, so problems do not occur when two different users create a filter with the same name. However, a single user or two

users who log into the default admin account should not create filters with the same name.

If users create filters with the same name, a conflict can occur under two conditions:

- Two users are logged into the default admin account on different sites and each creates a filter with the same name.
- One user creates a filter, logs into a different site, and immediately creates a filter with the same name.

If either condition occurs before site replication takes place, the user subsequently sees two filters with the same name in the filter list. Only one of the filters is usable. If this problem occurs, it is a best practice to delete the usable filter and recreate it with a different name. When you delete the usable filter, you also delete the unusable filter.

## Basic filter settings for logs

Most logs have the same Basic Settings.

[Table 11-3](#) describes the Basic Settings that are common to most logs.

**Table 11-3** Basic Settings for logs

Setting	Description
Log type	<p>Specifies the type of log you want to view.</p> <p>Select from the following types:</p> <ul style="list-style-type: none"> <li>■ Application and Device Control</li> <li>■ Audit</li> <li>■ Compliance</li> <li>■ Computer Status</li> <li>■ Network Threat Protection</li> <li>■ TruScan Proactive Threat Scan</li> <li>■ Risk</li> <li>■ Scan</li> <li>■ System</li> </ul>
Log content	<p>If there is more than one log of that type, you can select the type of log content you want to view.</p>
Use a saved filter	<p>Specifies which filter you want to use to create the log view.</p> <p>You can use the default filter or a custom filter that you have named and saved for viewing log information.</p>



**Table 11-3** Basic Settings for logs (*continued*)

Setting	Description
Time range	<p>Specifies the time range of events you want to view in the log.</p> <p>Select from the following times:</p> <ul style="list-style-type: none"><li>■ Past 24 hours</li><li>■ Past week</li><li>■ Past month</li><li>■ Current month</li><li>■ Past three months</li><li>■ Past year</li><li>■ Set specific dates</li></ul>
Advanced settings	<p>Each log has some advanced settings that are specific to it. Click Advanced Settings and Basic Settings to toggle back and forth between them.</p>

## Advanced filter settings for logs

Advanced settings provide additional control over the data that you want to view. They are specific to the log type and content.

If you have computers in your network that are running legacy versions of Symantec AntiVirus, then when you use log filters, the following terminology applies:

- Legacy server groups are categorized as domains
- Legacy client groups are categorized as groups
- Legacy parent servers are categorized as servers

---

**Note:** You cannot filter on Symantec Client Firewall legacy data for Intrusion Prevention signatures. To see the signature versions that run on a computer, you can go to the Computer Status log. Select a computer that has Symantec Client Firewall installed, and then click Details. The IDS version field contains this information.

---

For a description of each configurable option, you can click Tell me more for that type of log on the console. Tell me more displays the context-sensitive Help.

## Running commands and actions from logs

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

You can also right-click a group directly from the Client page of the console to run commands. The order in which commands and actions are processed on the client differs from command to command. Regardless of where the command is initiated, commands and actions are processed in the same way.

For information about the options you can set when you run commands, in the console on the Logs tab, you can click Tell me more. Clicking Tell me more displays the context-sensitive Help.

From the Command Status tab, you can view the status of the commands that you have run from the console and their details. You can also cancel a specific scan from this tab if the scan is in progress.

You can cancel all scans in progress and queued for selected clients from the Computer Status log. If you confirm the command, the table refreshes and you see that the cancel command is added to the command status table.

---

**Note:** If you run scan command, and select a Custom scan, the scan uses the command scan settings that you configured on the Administrator-defined Scan page. The command uses the settings that are in the Antivirus and Antispyware Policy that is applied to the selected clients.

If you run a Restart Computer command from a log, the command is sent immediately. If users are logged onto the client, they are warned about the restart based on the restart the options that the administrator configured for that client. You can configure client restart options on the General Settings tab of the General Settings dialog box under Settings on the Clients page.

---

The following logs allow you to add exceptions to a Centralized Exceptions Policy:

- Application Control log
- TruScan Proactive Threat Scan log
- Risk log

See [“Creating centralized exceptions from log events”](#) on page 540.

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

See [“Configuring a Centralized Exceptions Policy”](#) on page 534.

From the Risk log, you can also delete files from the Quarantine.

If Symantec Endpoint Protection detects risks in a compressed file, the compressed file is quarantined as a whole. However, the Risk log contains a separate entry for each file in the compressed file. You cannot use the Delete from Quarantine command from the Risk log to delete only the infected files from the Quarantine. To successfully delete the risk or risks, you must select all the files in the compressed file before you use the Delete from Quarantine command.

---

**Note:** To select the files in the compressed file, you must display them all in the log view. You can use the Limit option in the Risk log filter's Advanced Settings to increase the number of entries in the view.

---

#### To delete files from the Quarantine from the Risk log

- 1 Click **Monitors**.
- 2 On the Logs tab, from the Log type list box, select the Risk log, and then click **View Log**.
- 3 Select an entry in the log that has a file that has been quarantined.
- 4 From the Action list box, select Delete from Quarantine.
- 5 Click **Start**.
- 6 In the dialog box that appears, click **Delete**.
- 7 In the confirmation dialog box that appears, click **OK**.

#### To delete a compressed file from the Quarantine from the Risk log

- 1 Click **Monitors**.
- 2 On the Logs tab, from the Log type list box, select the Risk log, and then click **View Log**.
- 3 Select all entries for files in the compressed file.  
You must have all entries in the compressed file in the log view. You can use the Limit option under Advanced Settings to increase the number of entries in the view.
- 4 From the Action list box, select Delete from Quarantine.
- 5 Click **Start**.
- 6 In the dialog box that appears, click **Delete**.
- 7 In the confirmation dialog box that appears, click **OK**.

### To run a command from the Computer Status log

- 1 Click **Monitors**.
- 2 On the Logs tab, from the Log type list box, select Computer Status.
- 3 Click **View Log**.
- 4 Select a command from the Action list box.
- 5 Click **Start**.

If there are settings choices for the command that you selected, a new page appears where you can configure the appropriate settings.

- 6 When you have finished configuration, click **Yes** or **OK**.
- 7 In the command confirmation message box that appears, click **Yes**.
- 8 In the Message dialog box, click **OK**.

If the command is not queued successfully, you may need to repeat this procedure. You can check to see if the server is down. If the console has lost connectivity with the server, you can log off the console and then log back on to see if that helps.

### To view command status details

- 1 Click **Monitors**.
- 2 On the Command Status tab, select a command in the list, and then click **Details**.

### To cancel a specific scan that is in progress

- 1 Click **Monitors**.
- 2 On the Command Status tab, click the **Cancel Scan** icon in the Command column of the scan command that you want to cancel.
- 3 When a confirmation that the command was queued successfully appears, click **OK**.

### To cancel all in-progress and queued scans

- 1 Click **Monitors**.
- 2 On the Logs tab, from the Log type list box, select Computer Status.
- 3 Click **View Log**.
- 4 Select one or more computers in the list, and then select **Cancel All Scans** from the command list.
- 5 Click **Start**.

- 6 When the confirmation dialog box appears, click **Yes** to cancel all in-progress and queued scans for the selected computers.
- 7 When a confirmation that the command was queued successfully appears, click **OK**.

## About reducing the volume of events sent to the logs

You can reduce the number of events that are sent to the antivirus and antispyware logs by configuring log handling parameters. These options are configured on a per-policy basis from your Antivirus and Antispyware Policy.

See [“Setting up log handling parameters in an Antivirus and Antispyware Policy”](#) on page 375.

## Exporting log data

You have several choices for exporting the data in your logs. You can export the data in some logs to a comma-delimited text file. You can export other logs' data to a tab-delimited text file that is called a dump file or to a Syslog server. Log data export is useful if you want to accumulate all logs from your entire network in a centralized location. Log data export is also useful if you want to use a third-party program such as a spreadsheet to organize or manipulate the data. You also might want to export the data in your logs before you delete log records.

When you export log data to a Syslog server, you must configure the Syslog server to receive those logs. To forward logs to third-party programs, you need to have the third-party program installed and on the network. For example, you can use Microsoft Excel to open the exported log files. Each field appears in a separate column, a separate log record in each line.

---

**Note:** You cannot restore the database by using exported log data.

---

## 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 the *drive*:\Program Files\Symantec\Symantec Endpoint Protection Manager\data\dump folder. Entries are placed in a .tmp file until the records are transferred to the text file.

If you do not have Symantec Network Access Control installed, some of these logs do not exist.

Table 11-4 shows the correspondence of the types of log data to the names of the exported log data files.

**Table 11-4** Log text file names for Symantec Endpoint Protection

Log Data	Text File Name
Server Administration	scm_admin.log
Server Application Control	agt_behavior.log
Server Client	scm_agent_act.log
Server Policy	scm_policy.log
Server System	scm_system.log
Client Packet	agt_packet.log
Client Proactive Threat	agt_proactive.log
Client Risk	agt_risk.log
Client Scan	agt_scan.log
Client Security	agt_security.log
Client System	agt_system.log
Client Traffic	agt_traffic.log

**Note:** The log names in Table 11-4 do not correspond one-to-one to the log names that are used on the Logs tab of the Monitors page.

Table 11-5 shows the correspondence of the types of log data to the names of the exported log data files for the Enforcer logs.

**Table 11-5** Additional log text file names for Symantec Network Access Control

Log Data	Text File Name
Server Enforcer Activity	scm_enforcer_act.log
Enforcer Client Activity	enf_client_act.log
Enforcer System	enf_system.log
Enforcer Traffic	enf_traffic.log

---

**Note:** When you export to a text file, the number of exported records can differ from the number you set in the External Logging dialog box. This situation arises when you restart the management server. After you restart the management server, the log entry count resets to zero, but there may already be entries in the temporary log files. In this situation, the first \*.log file of each type that is generated after the restart contains more entries than the specified value. Any log files that are subsequently exported contain the correct number of entries.

---

For more information about the options you can set in this procedure, you can click Help on the console for the General tab.

#### To export log data to a dump file

- 1 In the console, click **Admin**.
- 2 Click **Servers**.
- 3 Click the local site or remote site that you want to configure external logging for.
- 4 Click **Configure External Logging**.
- 5 On the General tab, select how often you want the log data to be sent to the file.
- 6 Select the Master Logging server that you want to handle external logging.  
If you use Microsoft SQL with more than one management server connecting to the database, only one server needs to be a Master Logging Server.
- 7 Check **Export logs to a dump file**.
- 8 If necessary, check **Limit dump file records** and type in the number of entries that you want to send at a time to the text file.
- 9 On the Log Filter tab, select all of the logs that you want to send to text files.  
If a log type that you select lets you select the severity level, you must check the severity levels that you want to save. All levels that you select are saved.
- 10 Click **OK**.

## Exporting data to a Syslog server

You can configure Symantec Endpoint Protection to send the log data from some logs to a Syslog server.

---

**Note:** Remember to configure your Syslog server to receive the log data.

---

For more information about the options you can set in this procedure, you can click **Help** on the console for the **General** tab.

#### To export log data to a Syslog server

- 1 In the console, click **Admin**.
- 2 Click **Servers**.
- 3 Click the local site or remote site that you want to export log data from.
- 4 Click **Configure External Logging**.
- 5 On the **General** tab, select how often you want the log data to be sent to the file.
- 6 Select the server you want to handle external logging.

If you use Microsoft SQL and have multiple management servers connected to the database, you only need one server to be the Master Logging Server.

- 7 Check **Enable Transmission of Logs to a Syslog Server**.
- 8 Configure the following fields as desired:
  - **Syslog Server:**  
Type in the IP address or domain name of the Syslog server that you want to receive the log data.
  - **UDP Destination Port:**  
Type in the destination port that the Syslog server uses to listen for Syslog messages or use the default.
  - **Log Facility:**  
Type in the number of the log facility that you want to be used in the Syslog configuration file or use the default. Valid values range from 0 to 23.
- 9 On the **Log Filter** tab, select all of the logs that you want to send to text files. If a log type that you select lets you select the severity level, check the severity levels that you want to save.
- 10 Click **OK**.

## Exporting log data to a comma-delimited text file

You can export the data in the logs to a comma-delimited text file.

#### To export logs to a comma-delimited text file

- 1 In the console, click **Monitors**.
- 2 On the **Logs** tab, select the log that you want to export.



- 3 Change any **Basic Settings** or **Advanced Settings**.
- 4 Click **View Log**.
- 5 Click **Export**.
- 6 In the new window that appears, click the **File** menu and then click **Save As**.
- 7 If you are prompted to continue, click **Yes**.
- 8 In the Save Web Page window that appears, use the Save in list box to browse to the directory where you want to save the file.
- 9 In the File name text box, type a file name to use.
- 10 To save the raw data, in the Save as type list box, change the type to **Text File (\*.txt)**.
- 11 Click **Save** to export the data to the file.

## Using notifications

Notifications are messages about the security events that have taken place in your network. You can configure many different types of notifications to occur. Some notifications are directed at users and some notifications are directed at administrators.

You can configure the following notification actions to alert administrators or other designated individuals when a number of different security-related conditions are met:

- Send an email.
- Run a batch file or another executable file.
- Log an entry in the notifications log in the database.

See [“Creating administrator notifications”](#) on page 195.

## Viewing and filtering administrator notification information

You can view the information from the notifications log in the same way that you view the information that is contained in other logs. You can filter the notifications log to view information about a single type of notification event at a time. You can filter your view of notifications and save the filters for future use.

You can filter notifications in the log based on the following criteria:

- Time range
- Acknowledgment status

- Type
- Creator
- Name

#### To view all notifications

- 1 In the console, click **Monitors**.
- 2 On the Notifications tab, click **View Notifications**.

The list of all types of notifications appears.

#### To filter your view of notifications

- 1 In the console, click **Monitors**.
- 2 On the Notifications tab, under **What filter settings would you like to use**, click **Advanced Settings**.
- 3 Set any option you want to filter on.

You can filter on any combination of the time range, the acknowledgment status, the notification type, the creator, or a specific notification name.

- 4 Click **View Notifications**.

A list of the type of notifications that you selected appears.

## Threshold guidelines for administrator notifications

Some notification types contain default values when you configure them. These guidelines provide reasonable starting points depending on the size of your environment, but they may need to be adjusted. Trial and error may be required to find the right balance between too many and too few notifications for your environment. Set the threshold to an initial limit, then wait for a few days. See if you receive notifications too infrequently or if notifications swamp you or your network.

For virus, security risk, and firewall event detection, suppose that you have fewer than 100 computers in a network. A reasonable starting point in this network is to configure a notification when two risk events are detected within one minute. If you have 100 to 1000 computers, detecting five risk events within one minute may be a more useful starting point.

You may also want to be alerted when clients have out-of-date definitions. You may want to be notified of each client that has a definitions file that is more than two days out of date.

## Creating administrator notifications

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

You can configure the software take the following notification actions:

- Log the notification to the database.
- Send an email to individuals.

---

**Note:** To send notifications by email, you must also configure a mail server. You can configure a mail server by using the Mail Server tab on the Admin Servers page.

---

- Run a batch file or other kind of executable file.

The default damper period for notifications is Auto (automatic). If a notification is triggered and the trigger condition continues to exist, the notification action that you configured is not performed again for 60 minutes. For example, suppose you set a notification so that you are emailed when a virus infects five computers within one hour. If a virus continues to infect your computers at or above this rate, Symantec Endpoint Protection emails you every hour. The emails continue until the rate slows to fewer than five computers per hour.

You can configure the software to notify you when the following types of events occur:

- **Authentication failure**  
Logon failures trigger this type of notification. You set the number of logon failures and the time period that you want to trigger a notification. Symantec Endpoint Protection notifies you if the number of logon failures that occur during the time period exceeds your setting. It reports the number of logon failures that occurred.
- **Client list change**  
Changes to the clients trigger this type of notification. The types of changes that can trigger this notification include the addition, movement, name change, or deletion of a client. Additional possibilities are that a client's Unmanaged Detector status, client mode, or hardware changed.
- **Client security alert**  
You can choose from compliance, Network Threat Protection, traffic, packet, device control, and application control security events. You can also choose the type and extent of the outbreak that should trigger this notification and the time period. Types include occurrences on any computer, occurrences on

a single computer, or occurrences on distinct computers. Some of these types require that you also enable logging in the associated policy.

- **Enforcer is down**  
An offline Enforcer appliance triggers this type of notification. The notification tells you the name of each Enforcers, its group, and the time of its last status.
- **Forced or Commercial application detected**  
The detection of an application on the Commercial Application List or on the administrator's list of applications to watch for triggers this notification.
- **New learned application**  
New learned applications trigger this type of notification.
- **New risk detected**  
New risks trigger this type of notification.
- **New software package**  
New software package downloads trigger this type of notification.
- **Risk outbreak**  
You set the number and type of occurrences of new risks and the time period that should trigger this type of notification. Types include occurrences on any computer, occurrences on a single computer, or occurrences on distinct computers.
- **Server health**  
Server health statuses of offline, poor, or critical trigger this notification. The notification lists the server name, health status, reason, and last status.
- **Single risk event**  
The detection of a single risk event triggers this notification. The notification lists a number of details about the risk, which includes the user and computer involved, and the action that Symantec Endpoint Protection took.
- **System event**  
System events such as server and Enforcer activities, replication failure, backup and restore problems, and system errors trigger this notification. The notification lists the number of such events that were detected.
- **Unmanaged computer**  
Unmanaged computers trigger this notification. The notification lists details such as the IP address, MAC address, and operating system for each computer.
- **Virus definitions out-of-date**  
You define out-of-date when setting up the notification. You set the number of computers and the number of days that the computer's definitions must be older than to trigger this notification.

Using the Notification Conditions settings, you can configure a client security alert by occurrences on any computer, a single computer, or on distinct computers. You can also configure these options for a risk outbreak.

See “[Configuring notifications for Network Threat Protection](#)” on page 475.

For a description of each configurable option, you can click Tell me more on the console. Tell me more displays the context-sensitive Help.

---

**Note:** You can filter your view of the Notification Conditions you have created by using the Show notification types list box. To be sure that the new notifications that you create are displayed, make sure that All is selected in this list box.

---

#### To create a notification

- 1 In the console, click **Monitors**.
- 2 On the Notifications tab, click **Notification Conditions**.
- 3 Click **Add**, and then select the type of notification that you want to add from the list that appears.
- 4 In the new window that appears, in the Notification name text box, type a descriptive name.
- 5 Specify the filter options that you want. For example, for some types of notifications, you can limit the notification to specific domains, groups, servers, computers, risks, or applications.
- 6 Specify the notification settings and the actions that you want to occur when this notification is triggered. You can click Help to see descriptions of the possible options for all types of notifications.

If you select **Send email to** as the action to take, the email notification depends on the mail server's user name option. The user name that is configured for the mail server from the Server Properties dialog must be of the form *user@domain*. If this field is left blank, the notifications are sent from *SYSTEM@computer name*. If the reporting server has a name that uses Double Byte Character Set (DBCS) characters, you must specify the user name field with an email account name of the form *user@domain*.

If you select **Run the batch or executable file** as the action to take, type in the name of the file. Path names are not allowed. The batch file or executable file to run must be located in the following directory:

*drive:\Program Files\Symantec\Symantec Endpoint Protection Manager\bin*

- 7 Click **OK**.

You may want to create a Network Threat Protection notification that is triggered when a traffic event matches the criteria that are set for a firewall rule.

To create this type of notification, you must perform the following tasks:

- In the Firewall Policy Rules list, check the Send Email Alert option in the Logging column of the rules you want to be notified about.
- On the Notifications tab, configure a Client security alert for Network Threat Protection, Packet, or Traffic events.

#### To create a Network Threat Protection notification

- 1 In the console, click **Monitors**.
- 2 On the Notifications tab, click **Notification Conditions**.
- 3 Click **Add** and select Client security alert.
- 4 Type in a name for this notification.
- 5 If you want to limit this notification to specific domains, groups, servers, or computers, specify the filter options that you want.
- 6 Select one of the following outbreak types:
  - Occurrences on distinct computers
  - Occurrences on any computer
  - Occurrences on single computer
- 7 To specify the type of Network Threat Protection activity, check one of the following check boxes:
  - For the attacks and events that the firewall detects or the Intrusion Prevention signatures detect, check **Network Threat Protection events**.
  - For the firewall rules that are triggered and recorded in the Packet Log, check **Packet events**.
  - For the firewall rules that are triggered and recorded in the Traffic Log, check **Traffic events**.
- 8 If desired, change the default notification conditions to set the number of occurrences within the number of minutes that you want to trigger this notification.

- 9 Check **Send email to**, and then type in the email addresses of the people that you want to notify when these criteria are met.
- 10 Click **OK**.

The Send Email Alert option in the Logging column of the Firewall Policy Rules list is now operational. When this notification is triggered, email is sent.

See [“Configuring email messages for traffic events”](#) on page 476.

## About editing existing notifications

If you edit the settings of an existing notification, the previous entries that it generated display messages in the notifications log based on your new settings. If you want to retain your past notification messages in the notifications log view, do not edit the settings of an existing notification. Instead, create a new notification with a new name. Then, disable the existing notification by unchecking the actions that you configured under What should happen when this notification is triggered.





# Using Monitors and Reports to help secure your network

This chapter includes the following topics:

- [About using Monitors and Reports to help secure your network](#)
- [About eliminating viruses and security risks](#)
- [Finding the clients that are offline](#)

## About using Monitors and Reports to help secure your network

Reports display a static snapshot of information about your clients and servers, but they can be scheduled to run at intervals to present up-to-date information. The logs that you access from the Monitors page are dynamic and display more specific and detailed information, such as computer and user names. You may need this level of detail to pinpoint some problems. You can run commands to all the clients in a group from some logs to immediately remediate problems. You can monitor the status of commands from the Command Status tab.

The notifications that you can set up from the Monitors page can alert you to problems. You can use a notification to trigger the remediation of a problem by having it run a batch file or other executable. You can set a notification to occur when certain events occur or reach a threshold number of occurrences.

You can get information of interest from the logs and reports in many different ways. For example, suppose you want to know which computers are infected in your network. The Home page shows a count for newly infected and still infected computers. This count tells you immediately when you log on to the console if security problems were found in your network.

You can find more details about these computers in many different ways. For example, you can do the following:

- Schedule the Infected and At Risk Computers quick report to run every morning and configure it to be emailed to yourself or another person.
- Construct and save a Risk report filter that includes the specific details that you want about infected computers. Run a quick report by using that filter whenever you see from the Home page that a security problem has occurred. Or, you can create a scheduled report to run that uses that saved filter and email it to yourself or another person.
- Go directly to the Risk log and view the infection events. You can use either the default filter or a saved filter with only the details that you want.
- Customize the Home page to change the default reports in the Favorite Reports section, if desired. You can use any predefined quick report or a report that uses a custom filter. These reports run whenever you view them so that the information they contain is current.

No matter what your preferred approach is, you may want to create some custom report and log filters. You can use custom filters on a regular basis to monitor or eliminate security problems in your network. To customize filters, you must first identify the information that you want to see in the report or log. For example, you can run a report to display the top security risks that infected your network over a specific time. Say you find that the top risk in your network last week was RPC.Attack. The report identifies how many computers were infected. You can then use the Risk log to display the names of the computers that were infected with RPC.Attack. The Risk log also shows the names of the users who were logged in to those computers at the time of infection.

## About the information in the Application Control and Device Control reports and logs

Application Control and Device Control logs and reports contain information about the following types of events:

- Access to a computer entity was blocked
- A device was kept off the network

Files, registry keys, and processes are examples of computer entities. The information that is available includes items such as the time and the event type; the action taken; the host, and the rule involved. It also contains the caller process that was involved. These logs and these reports include information about the Application and Device Control Policies and Tamper Protection.

[Table 12-1](#) describes some typical uses for the kind of information that you can get from Application Control and Device Control reports and logs.

**Table 12-1** Application Control and Device Control quick reports and logs summary

Report or log	Typical uses
Top Groups with most Alerted Application Control Logs	Use this report to check which groups are most at risk in your network.
Top Targets Blocked	Use this report to check which files, processes, and other entities are used most frequently in attacks against your network.
Top Devices Blocked	Use this report to find out which devices are the most problematic from the standpoint of compromising your network's security.
Application Control log	Use this log to see information about the following entities: <ul style="list-style-type: none"><li>■ The actions that were taken in response to events</li><li>■ The processes that were involved in the events</li><li>■ The rule names that were applied from the policy when an application's access is blocked</li></ul>
Device Control log	Use this log when you need to see Device Control details, such as the exact time that Device Control enabled or disabled devices. This log also displays information such as the name of the computer, its location, the user who was logged on, and the operating system involved.

## About the information in the Audit report and log

The Audit log contains information about policy modification activities, such as the event times and types, policy modifications, domains, sites, administrators, and descriptions.

The default Audit quick report is called Policies Used. View the Policies Used report to monitor the policies in use in your network, by group. You can look at the Audit log when you want to see which administrator changed a particular policy and when.

## About the information in the Compliance reports and logs

The Compliance logs contain information about the Enforcer server, clients, and traffic, and about host compliance. The information available includes items such as the time and the event type, the name of the Enforcer involved, the site, and the server.

---

**Note:** If you do not have Symantec Network Access Control installed, the Compliance logs and reports do not contain any data.

---

[Table 12-2](#) describes some typical uses for the kind of information that you can get from Compliance reports and logs.

**Table 12-2** Compliance logs and quick reports summary

Report or log	Typical uses
Network Compliance Status	Use this report to look at overall compliance, to see if clients have failed host integrity checks or authentication, or have been disconnected.
Compliance Status	Use this report to see the total number of clients that have either passed or failed a host integrity check in your network.
Clients by Compliance Failure Summary	Use this report to see the general reasons for control failure events, such as antivirus, firewall, or VPN.
Compliance Failure Details	Use this report to see a greater level of detail about the compliance failures. It shows the criteria and the rule that was involved in each failure. It includes the percentage of clients that have been deployed and the percentage that failed.  For example, the Compliance Failure Summary can show ten client failures due to the antivirus software. In contrast, Compliance Failure Details shows the following information: <ul style="list-style-type: none"><li>■ Four clients have no antivirus software currently in operation on them.</li><li>■ Two clients have no antivirus software installed.</li><li>■ Four clients have out-of-date antivirus definitions files.</li></ul>
Non-compliant Clients by Location	Use this report to see if some locations have more compliance problems than the others.

**Table 12-2** Compliance logs and quick reports summary (*continued*)

Report or log	Typical uses
Enforcer Server log	<p>Use this log to look at information about Enforcer compliance events, the name of the Enforcer involved, its site, and its server.</p> <p>Among other things, this log contains the following information:</p> <ul style="list-style-type: none"> <li>■ Which Enforcers were unable to register with their servers</li> <li>■ Which Enforcers have successfully received downloads of policies and the sylink.xml communication file</li> <li>■ Whether or not the Enforcers' server has successfully received the Enforcers' logs</li> </ul>
Enforcer Client log	<p>Use this log to see which clients have passed or failed Host Integrity checks, were authenticated or rejected, or were disconnected from the network.</p>
Enforcer Traffic log	<p>Use this log to look at information about the traffic that moves through an Enforcer.</p> <p>The information available includes:</p> <ul style="list-style-type: none"> <li>■ The direction of the traffic</li> <li>■ The time when the traffic began and the time when the traffic ended</li> <li>■ The protocol used</li> <li>■ The source IP address and destination IP address that was used</li> <li>■ The port that was used</li> <li>■ The packet size (in bytes)</li> <li>■ The attempted connections that were allowed or blocked</li> </ul> <p>This log applies only to Gateway Enforcers.</p>
Host Compliance log	<p>Use this log to look at specific information about particular compliance events. Such events include the reason, the user involved, and the name of the operating system that was involved.</p>

## About the information in the Computer Status reports and log

The Computer Status log contains information about the real-time operational status of the computers in the network. Information available includes the computer name and IP address, last check-in time, definitions date, infected status, Auto-Protect status, server, group, domain, and user name. Filters for Computer Status reports have both standard configuration options and compliance-specific options.

[Table 12-3](#) describes some typical uses for the kind of information that you can get from Computer Status reports and logs.

**Table 12-3** Computer Status quick reports and log summary

Report or log	Typical uses
Virus Definitions Distribution	Use this report to make sure that all the groups, domains, or servers in your network use up-to-date virus definitions files versions.
Computers Not Checked into Server	Use this report to find the computers that have not checked in with a server and therefore might be lost or missing.
Symantec Endpoint Protection Product Versions	Use this report to check the versions of product software, virus definitions, IPS signatures, and proactive protection content in use in your network. With this information you can pinpoint the computers that need an update.
Intrusion Prevention Signature Distribution	Use this report to make sure that all the groups your network use up-to-date intrusion prevention signatures. You can also see which domains or servers are out-of-date.
Client Inventory	Use this report to see the number and percentage of computers that fall into certain hardware and software categories. Available information includes the computers' operating system, total memory, free memory, total disk space, free disk space, and processor type. For example, from the Client Inventory report, you might see that 22% of your computers have less than 1 GB of free disk space.
Compliance Status Distribution	Use this report to see which groups or subnets have the largest percentage of computers out of compliance. You may want to investigate if certain groups seem to have a lot more compliance problems than others.

**Table 12-3** Computer Status quick reports and log summary (*continued*)

Report or log	Typical uses
Client Online Status	Use this report to see which groups or subnets have the largest percentage of clients online. You may want to investigate why some groups or subnets currently experience more problems than others.
Clients With Latest Policy	Use this report to see which groups or subnets have the largest percentage of computers that don't have the latest policy on them.
Client Count by Group	Use this report to see the total number of clients and users, by group.
Security Status Summary	<p>Use this report to quickly see the total number of computers that have the following problems:</p> <ul style="list-style-type: none"> <li>■ Auto-Protect is disabled</li> <li>■ The antivirus engine is turned off</li> <li>■ Tamper Protection is turned off</li> <li>■ The computer needs to be restarted</li> <li>■ The computer failed a host integrity check</li> <li>■ Network Threat Protection is turned off</li> </ul> <p>These computers may continue to be at risk unless you intervene.</p>
Protection Content Versions	Use this report to check the versions of Proactive Protection content in use in your network, to pinpoint any computers that need an update.
Client Migration	Use this report to see the migration status of clients by domain, group, and server. You can quickly identify clients where migration has failed or has not yet started.
Clients Online/ Offline Over Time (Snapshots)	Use this report to pinpoint the clients that don't connect to the network frequently enough. This report is available only as a scheduled report.
Clients With Latest Policy over Time (Snapshots)	Use this report to pinpoint the clients that don't get policy updates frequently enough. This report is available only as a scheduled report.
Client Software Rollout (Snapshots)	Use this report to pinpoint the clients that don't have the latest software version deployed. This report is available only as a scheduled report.

**Table 12-3** Computer Status quick reports and log summary (*continued*)

Report or log	Typical uses
Non-compliant Clients Over Time (Snapshots)	Use this report to pinpoint the clients that frequently fail host integrity checks. This report is available only as a scheduled report.
Virus Definitions Rollout (Snapshots)	Use this report to check to see the definitions versions that clients have. This report is available only as a scheduled report.
Computer Status log	Check the Computer Status log if you need more details about any of the areas that the reports cover.

## About the information in the Network Threat Protection reports and logs

Network Threat Protection logs allow you to track a computer’s activity and its interaction with other computers and networks. They record information about the traffic that tries to enter or exit the computers through their network connections.

Network Threat Protection logs contain details about attacks on the firewall, such as the following information:

- Denial-of-service attacks
- Port scans
- Changes that were made to executable files

Network Threat Protection logs collect information about intrusion prevention. They also contain information about the connections that were made through the firewall (traffic), the registry keys, files, and DLLs that are accessed. They contain information about the data packets that pass through the computers. The operational changes that were made to computers are also logged in these logs. This information may include when services start and stop or when someone configures software. Among the other types of information that may be available are items such as the time and the event type and the action taken. It can also include the direction, host name, IP address, and the protocol that was used for the traffic involved. If it applies to the event, the information can also include the severity level.

[Table 12-4](#) describes some typical uses for the kind of information that you can get from Network Threat Protection reports and logs.



**Table 12-4** Network Threat Protection quick reports and logs summary

Report or log	Typical uses
Top Targets Attacked	Use this report to identify which groups, subnets, computers, or ports are attacked most frequently. You may want to take some action based on this report. For example, you might find that the clients that attach through a VPN are attacked much more frequently. You might want to group those computers so that you can apply a more stringent security policy.
Top Sources of Attack	Use this report to identify which hosts attack your network most frequently.
Top Types of Attack	Use this report to identify the types of attack that are directed at your network most frequently. The possible types of attack that you can monitor include port scans, denial-of-service attacks, and MAC spoofing.
Top Blocked Applications Blocked Applications Over Time	Use these reports together to identify the applications that are used most frequently to attack your network. You can also see whether or not the applications being used for attacks have changed over time.
Attacks over Time	Use this report to identify the groups, IP addresses, operating systems, and users that are attacked most frequently in your network. Use it to also identify the most frequent type of attack that occurs.
Security Events by Severity	Use this report to see a summary of the severity of security events in your network.
Top Traffic Notifications Traffic Notifications Over Time	These reports show the number of attacks that violated the firewall rules that you configured to notify you about violations. You configure this data to be reported by checking the Send Email Alert option in the Logging column of the Firewall Policy Rules. Use Traffic Notifications Over Time to see how the attacks increase or decrease or affect different groups over time. Use them to see which groups are most at risk of attack through the firewall.
Full Report	Use this report to see the information that appears in all the Network Threat Protection quick reports in one place.

**Table 12-4** Network Threat Protection quick reports and logs summary  
*(continued)*

Report or log	Typical uses
Traffic log	Use this log if you need more information about a specific traffic event or type of traffic that passes through your firewall.
Packet log	Use this log if you need more information about a specific packet. You may want to look at packets to more thoroughly investigate a security event that was listed in a report.
Attacks log	Use this log if you need more detailed information about a specific attack that occurred.

## About the information in the TruScan proactive threat scan reports and logs

[Table 12-5](#) describes some typical uses for the kind of information that you can get from TruScan proactive threat scan reports and log.

**Table 12-5** TruScan proactive threat scan quick reports and logs summary

Report or log	Typical uses
TruScan Proactive Threat Scan Detection Results (located under Risks reports)  TruScan Proactive Threat Detection Over Time (located under Risks reports)	<p>Use this report to see the following information:</p> <ul style="list-style-type: none"> <li>■ A list of the applications that are labeled as risks that you have added to your exceptions as acceptable in your network</li> <li>■ A list of the applications that have been detected that are confirmed risks</li> <li>■ A list of the applications that have been detected but whose status as a risk is still unconfirmed</li> </ul> <p>Use TruScan Proactive Threat Detection Over Time to see if the threats detected by TruScan proactive threat scans have changed over time.</p>

**Table 12-5** TruScan proactive threat scan quick reports and logs summary  
(continued)

Report or log	Typical uses
TruScan Proactive Threat Distribution (located in Risks reports)	<p>Use this report for the following reasons:</p> <ul style="list-style-type: none"> <li>■ To see which applications from the Commercial Applications List and Forced Detections list are detected most frequently</li> <li>■ To see what action was taken in response to the detection</li> <li>■ To determine if particular computers in your network are attacked more frequently by this vector</li> <li>■ To see details about the application that attacked</li> </ul>
TruScan Proactive Threat Scan log	<p>Use this log if you need more information about specific proactive threat detection events. This information can be something like the name of the user that was logged on when the detection occurred. You can also use commands from this log to add legitimate entities such as files, folders, extensions, and processes to the Centralized Exceptions Policy. After they are added to the list, if a legitimate activity is detected as a risk, the entity is not acted upon.</p>

## About the information in the Risk reports and log

The Risk log and reports include information about risk events on your management servers and their clients.

[Table 12-6](#) describes some typical uses for the kind of information that you can get from Risk quick reports and log.

**Table 12-6** Risk quick reports and log summary

Log and report types	Typical uses
Infected and At Risk Computers	Use this report to quickly identify the computers that need your attention because they are infected with a virus or a security risk.
Detection Action Summary	Use this report to identify the actions that were taken when risks were detected. This information also appears on the Symantec Endpoint Protection Home page.

**Table 12-6** Risk quick reports and log summary (*continued*)

Log and report types	Typical uses
Risk Detections Count	Use this report to identify the domains, groups, or particular computers that have the largest number of risk detections. You can then investigate why some entities seem to be at greater risk than others in your network.
New Risks Detected in the Network	Use this report to identify and track the impact of new risks on your network.
Top Risk Detections Correlation	Use this report to look for correlations between risks and computers, users, domains, and servers.
Risk Distribution Summary Risk Distribution Over Time	Use these reports to track the distribution of risks. You can also use it to pinpoint particular risks, domains, groups, servers, computers, and the users that seem to have more problems than others. You can use Risk Distribution Over Time to see how these risks change over time.
Action Summary for Top Risks	Use this report to review the actions that were taken on the risks that Symantec Endpoint Protection has detected in your network.
Number of Notifications Number of Notifications Over Time	Use these reports to refine how you create and configure notifications in your network.
Weekly Outbreaks	Use this report to track risk outbreaks week by week.
Comprehensive Risk Report	Use this report to see all of the distribution reports and the new risks report information at one time.
Risk log	Use this log if you need more specific information about any of the areas in the Risk reports. For example, you can use the Risk log to see details about the risks that were detected on the computers where risks are often found. You can also use the Risk log to see details about security risks of a particular severity that have affected your network.

## About the information in the Scan reports and log

The Scan reports and log contain information about antivirus and antispyware scan activity.

[Table 12-7](#) describes some typical uses for the kind of information that you can get from Scan quick reports and log.

**Table 12-7** Scan quick reports and logs summary

Report or log	Typical uses
Scan Statistics Histogram	Group by scan time when you use this report to see a histogram of how long it takes for scheduled scans to complete on clients. You might want to change the time the scan is scheduled for based on this information. You can filter this report based on the number of files that were scanned. These results can help you to see if any users restrict the scans to a small number of files on their computers.
Computers by Last Scan Time	Use this report to identify the computers that have not run a scan recently. You can configure it to look for the last day or the last week or a custom time period that you want to check.
Computers Not Scanned	Use this report to get a list of the computers that have not been scanned for a specific time period. This report also tells you the computers' IP addresses by specific domains or by groups. These computers may be at risk.
Scan log	You can sort this log by scan duration to identify the computers that take the longest time to scan in your network. Based on this information, you can customize scheduled scans for these computers if needed.

## About the information in the System reports and logs

The System logs contain information that is useful for troubleshooting client problems.

[Table 12-8](#) describes some typical uses for the kind of information that you can get from System quick reports and log.

**Table 12-8** System Log and quick reports summary

Report or log	Typical uses
Top Clients That Generate Errors	Use this report to see which clients generate the largest number of errors and warnings. You may want to look at the location and type of users on these clients to see why they experience more problems than others. You can then go to the System log for details.

**Table 12-8** System Log and quick reports summary (*continued*)

Report or log	Typical uses
Top Servers That Generate Errors	Use this report to see which servers generate the largest number of errors and warnings. You may want to look at these servers to see why they experience more problems than is typical for your network.
Top Enforcers That Generate Errors	Use this report to see which Enforcers generate the largest number of errors and warnings. You may want to look at these Enforcers to see why they experience more problems than is typical for your network.
Database Replication Failures Over Time	Use this report to see which servers or sites experience the most problems with database replication. It also tells you why the replications fail so that you can remediate the problems.
Site Status	Use this report to see how your server handles its client load. Based on the information that is in this report, you may want to adjust the load.
Administrative log	<p>Use this log to look at administrative-related items like the following activities:</p> <ul style="list-style-type: none"> <li>■ Logons and logoffs</li> <li>■ Policy changes</li> <li>■ Password changes</li> <li>■ When certificates are matched</li> <li>■ Replication events</li> <li>■ Log-related events</li> </ul> <p>This log may be useful for troubleshooting client problems such as missing certificates, policies, or imports. You can look separately at events as they relate to domains, groups, users, computers, imports, packages, replications, and other events.</p>
Client-Server Activity log	<p>Use this log to look at all the client activity that takes place for a specific server.</p> <p>For example, you can use this log to look at the following items:</p> <ul style="list-style-type: none"> <li>■ Successful and unsuccessful policy downloads</li> <li>■ Client connections to the server</li> <li>■ Server registrations</li> </ul>

**Table 12-8** System Log and quick reports summary (*continued*)

Report or log	Typical uses
Server Activity log	<p>Among other things, use this log for the following reasons:</p> <ul style="list-style-type: none"><li>■ To locate and troubleshoot replication problems</li><li>■ To locate and troubleshoot backup problems</li><li>■ To locate and troubleshoot Radius Server problems</li><li>■ To look at all server events of a particular severity level</li></ul>
Client Activity log	<p>Among other things, you can use this log to monitor the following client-related activities:</p> <ul style="list-style-type: none"><li>■ Which clients have been blocked from accessing the network</li><li>■ Which clients need to be restarted</li><li>■ Which clients had successful or unsuccessful installations</li><li>■ Which clients had service initiation and termination problems</li><li>■ Which clients had rules import problems</li><li>■ Which clients had problems downloading policies</li><li>■ Which clients had failed connections to the server</li></ul>
Enforcer Activity log	<p>Use this log to monitor problems with the Enforcers. In this log, you can view management events, Enforcer events, enable events, and policy events. You can filter them by their severity level.</p> <p>For example, you can use this log to troubleshoot the following types of problems:</p> <ul style="list-style-type: none"><li>■ Enforcer connectivity</li><li>■ The importation and application of policies and configurations</li><li>■ Enforcer starts, stops, and pauses</li></ul>

---

**Note:** If you do not have Symantec Network Access Control installed, the Enforcer Activity log and the entries in other logs that apply to Enforcers are empty.

---

## About eliminating viruses and security risks

Eliminating virus infections and security risks is a task you can perform either every day or as needed, depending on your network's security status. First, you identify and locate the risks, then decide how to handle them. After you remediate problems, you can update the Computer Status log to show that you have responded to the risks.

### Identifying the infected and at risk computers

The first task is to identify the computers that are infected and at risk.

#### To identify infected computers

- 1 In the console, click **Home** and look at the Action Summary.

If you are a system administrator, you see counts of the number of Newly Infected and Still infected computers in your site. If you are a domain administrator, you see counts of the number of Newly Infected and Still infected computers in your domain. Still Infected is a subset of Newly Infected, and the Still Infected count goes down as you eliminate the risks from your network. Computers are still infected if a subsequent scan would report them as infected. For example, Symantec Endpoint Protection might have been able to clean a risk only partially from a computer and thus Auto-Protect still detects the risk.

- 2 In the console, click **Reports**.
- 3 In the Report type list box, click **Risk**.
- 4 In the Select a report list box, click **Infected and At Risk Computers**.
- 5 Click **Create Report** and note the lists of the infected and at risk computers that appear.

### Changing an action and rescanning the identified computers

The next step in the remediation of the risks in your network is to identify why the computers are still infected or at risk. Check the action that was taken for each risk on the infected and at risk computers. It may be that the action that was configured and taken was Left Alone. If the action was Left Alone, you should either clean the risk from the computer, remove the computer from the network, or accept the risk. You may want to edit the Antivirus and Antispyware Policy that is applied to the group that this computer is in. You may want to configure a different action for this category of risks, or for this specific risk.



### To identify the actions that need to be changed and rescan the identified computers

- 1 In the console, click **Monitors**.
- 2 In the Logs tab, select the Risk log, and then click **View Log**.

From the Risk log event column, you can see what happened and the action that was taken. From the Risk Name column, you can see the names of the risks that are still active. From the Domain Group User column you can see which group the computer is a member of.

If a client is at risk because a scan took the action Left Alone, you may need to change the Antivirus and Antispyware Policy for the group. From the Computer column, you can see the names of the computers that still have active risks on them.

See [“Configuring actions for known virus and security risk detections”](#) on page 384.

If your policy is configured to use Push mode, it is pushed out to the clients in the group at the next heartbeat.

See [“Specifying push or pull mode”](#) on page 340.

- 3 Click **Back**.
- 4 In the Logs tab, select the Computer Status log, and then click **View Log**.
- 5 If you changed an action and pushed out a new policy, select the computers that need to be rescanned with the new settings.
- 6 From the Command list box, select Scan, and then click **Start** to rescan the computers.

You can monitor the status of the Scan command from the Command Status tab.

## Restarting the computers that need a restart to finish remediation

Computers may still be at risk or infected because they need to be restarted to finish the remediation of a virus or security risk.

### To restart computers to finish remediation

- 1 In the Risk log, check the Restart Required column.  
It may be that a risk was partially cleaned from some computers, but the computers still require a restart to finish the remediation.
- 2 Select the computers in the list that require a restart.
- 3 In the Command list box, select Restart Computers, and then click **Start**.  
You can monitor the status of the Restart Computers command from the Command Status tab.

## Updating definitions and rescanning

Some computers can still be at risk because their definitions are out-of-date.

### To update definitions and rescan

- 1 For the remaining computers in the view, check the Definitions Date column. If some computers have virus definitions that are out of date, select those computers.
- 2 In the Command list box, select Update Content and Scan, and then click **Start**.  
You can monitor the status of the Update Content and Scan command from the Command Status tab.
- 3 Click **Home** and look at the numbers in the Action Summary Still Infected and Newly Infected rows.  
If the counts are zero, you have eliminated the risks. If the counts are not zero, you should investigate the remaining risks.

## About investigating and cleaning the remaining risks

If any risks remain, you may need to investigate them further. From the scan results dialog box, you can click the link to Symantec Security Response for the detected risk. The scan results also tell you what processes, files, or registry keys are involved in the risk detection. You may be able to create a custom Application Control policy to block an offending application. Or, you may need to disconnect the computer from the network and delete files and registry keys and stop processes manually.

## Eliminating the suspicious events

A suspicious security risk indicates that a TruScan proactive threat scan has detected something that you should investigate. It may or may not be harmless. If you determine that this risk is harmless, you can use the Centralized Exceptions Policy to exclude it from detection in the future. If the proactive threat scans cannot remediate a risk or if you have configured it to leave a risk alone, you may need to eliminate those risks.

If you configured TruScan proactive threat scans to log, and you investigate and determine that a risk is harmful, you can remediate it with the Centralized Exceptions Policy. Configure the Centralized Exceptions Policy to terminate or quarantine the risk instead of logging it.

If Symantec Endpoint Protection detected this risk by using the default TruScan proactive threat scan settings, then Symantec Endpoint Protection cannot remediate this risk. If you determine that this risk is harmful, you should remove the risk manually. After you have removed the risk, you can delete that entry from the Risk log.

## Finding the clients that are offline

You can check to see which computers are offline in your network in several ways. For example, you can perform the following checks:

- Run the Computer Status quick report Computers Not Checked into Server to see online status.
- Configure and run a custom version of this report to look at the computers in a particular group or site.
- View the Computer Status log, which contains the computer's IP address, and time of last check-in.

A client may be offline for a number of reasons. You can identify the computers that are offline and remediate these problems in a number of ways.

If you have Symantec Network Access Control installed, you can use the Compliance filter options to customize the Computers Not Checked into Server quick report. You can then use this report to look at the specific reasons that computers are not on the network. You can then eliminate the problems that you see.

Among the compliance reasons you can filter on are the following reasons:

- The computer's antivirus version is out-of-date.
- The computer's antivirus software is not running.

- A script failed.
- The computer's location has changed.

**To find the clients that are offline**

- 1 In the console, click **Monitors**.
- 2 On the Logs tab, from the Log type list box, click **Computer Status**.
- 3 Click **Advanced Settings**.
- 4 In the Online status list box, click **Offline**.
- 5 Click **View Log**.

By default, a list of the computers that have been offline for the past 24 hours appears. The list includes each computer's name, IP address, and the last time that it checked in with its server. You can adjust the time range to display offline computers for any time range you want to see.

# Advanced administrative tasks

- [Managing single and multiple company sites](#)
- [Managing servers](#)
- [Managing directory servers](#)
- [Managing email servers](#)
- [Managing proxy servers](#)
- [Managing RSA servers](#)
- [Managing server certificates](#)
- [Managing databases](#)
- [Replicating data](#)
- [Managing Tamper Protection](#)



# Managing single and multiple company sites

This chapter includes the following topics:

- [About the management of sites](#)
- [What you can do at a site](#)
- [What you cannot do at a site](#)
- [About site replication across different company sites](#)
- [About optional Enforcers at a site](#)
- [About remote sites](#)
- [Editing site properties](#)
- [Backing up a site](#)
- [Deleting remote sites](#)

## About the management of sites

Symantec organizes installations of components into sites. A site comprises single or multiple Symantec Endpoint Protection Managers and one database (MS SQL or embedded). It optionally includes one or more Enforcers that are typically located together at the same business location. Large enterprise corporations typically install many sites. The number of sites that are needed may be related to the company having multiple physical locations, separate divisions, and areas on different subnets. Corporate management and IT departments are typically responsible for determining the number and location of these sites.

The local site is the Symantec Endpoint Protection Manager console that you are logged on to. This site can be located in another city. However, it does not necessarily mean that the site is physically local. Remote sites are the sites linked to the local site as a replication partner.

Centralized security management is possible from any Symantec Endpoint Protection Manager console where you can manage both local sites and remote sites.

## What you can do at a site

From a particular site, you can perform tasks such as the following on all sites (local and remote):

- Change a site description.  
See [“Editing site properties”](#) on page 226.
- Set the Symantec Endpoint Protection Manager console to log off after some period of time.  
See [“Editing site properties”](#) on page 226.
- Clear the clients that have not connected for a while.  
See [“Editing site properties”](#) on page 226.
- Set up log thresholds.
- Schedule daily and weekly reports.
- Configure external logging to filter and send logs to a file or to a Syslog server.
- Change a database name and description.  
See [“Editing the name and description of a database in the Symantec Endpoint Protection Manager console”](#) on page 271.

From a particular site, you can perform tasks such as the following only for a local site:

- Back up the local site immediately.  
See [“Backing up a Microsoft SQL database”](#) on page 263.  
See [“Backing up an embedded database on demand from the Symantec Endpoint Protection Manager”](#) on page 268.
- Change the backup schedule.  
See [“Scheduling automatic database backups from the Symantec Endpoint Protection Manager”](#) on page 269.
- Delete a selected server (only if you have multiple Symantec Endpoint Protection Managers connected to a single Microsoft SQL database).



- Add a connection to a replication partner in the same site.  
See [“Adding replication partners and schedule”](#) on page 292.
- Update the server certificate.  
See [“About server certificate types”](#) on page 253.
- Query the database for information.

These lists are not complete. They are meant to give you an idea of the types of tasks that you can perform locally or remotely.

## What you cannot do at a site

You cannot perform some tasks at a remote site.

If you want to install a new site, you need to go to a specific computer on which you installed a Symantec Endpoint Protection Manager, or an Enforcer. However, you can log onto a site remotely to perform other tasks that can only be performed on the Symantec Endpoint Protection Manager console of a local site.

See [“Logging on to the Symantec Endpoint Protection Manager”](#) on page 29.

## About site replication across different company sites

After the installation of the first site at a company, you can install additional sites as replication partners. You can add replication partners when installing the second and subsequent sites.

See the *Installation Guide for Symantec Endpoint Protection and Symantec Network Access Control* for more information on how to configure the first site during the initial installation.

## About optional Enforcers at a site

If you want additional enforcement at your site, you can install Gateway, LAN, and DHCP Enforcers.

If you want to add Enforcers to an existing site, see the *Symantec Network Access Control Enforcer Appliance Implementation Guide*.

## About remote sites

You can view other sites from the Servers tab. If you are connected to the other Symantec Endpoint Protection Manager consoles, you can also edit server properties of the remote site. You can perform the following tasks on remote sites:

- Delete a remote site and its replication partners.
- Change the remote server description.
- Change access to the remote site's Symantec Endpoint Protection Manager console.
- Set up an email server for a remote site.
- Schedule directory server synchronization for a remote site.
- Set up a connection from the remote site's server to a proxy server.
- Configure external logging to send logs to a file or a Syslog server.

## Editing site properties

Site properties include the following:

- Site name and site description
- Specifying the time period for when the console times out
- Whether or not to delete the clients that have not connected after some period of time
- Whether or not application learning is turned on for the site
- Maximum log sizes that are maintained at the site
- Report scheduling

You can edit local or remote site properties from the console.

### To edit site properties

- 1 In the Symantec Endpoint Protection Manager console, click **Admin**.
- 2 In the Admin page, under Tasks, click **Servers**.
- 3 In the Admin page, under View, expand **Local Site** (*Site site name*) or expand **Remote Sites**.
- 4 Select the site whose properties you want to edit.
- 5 In the Admin page, under Tasks, click **Edit Site Properties**.
- 6 In the Site Properties dialog box on the General tab, edit the description for the site in the Description box.

You can use up to 1024 characters.

- 7 In the Site Properties dialog box on the General tab, select a value from 5 minutes to Never from the Console Timeout list.  

The default is one (1) hour. The administrator is automatically logged off the console when the Console Timeout period is reached.
- 8 In the Site Properties dialog box on the General tab, check **Delete clients that have not connected for  $x$  days**.  

You can delete the users that have not connected for a specified number of days (from 1 to 99999). The default setting is enabled for a period of thirty (30) days.
- 9 In the Site Properties dialog box on the General tab, check **Keep track of every application that the clients run**.  

Learned applications help administrators track a client's network access and the use of applications by recording all applications that are started on each client. You can enable or disable the learning of applications for a specific site. If this option is not enabled, then tracking of applications does not occur for that site. Tracking of applications also no longer occurs even if it is enabled for those clients that connect to the designated site. This option functions like a master switch.
- 10 In the Site Properties dialog box on the General tab, select a reporting server from the Select a server to send notifications and run scheduled reports list.  

This option is only relevant if you use a Microsoft SQL database that is connected to multiple databases.
- 11 Click **OK**.

## Backing up a site

When you back up information about a site, you perform the same task as you do when you back up a database for a site.

See [“Backing up a Microsoft SQL database”](#) on page 263.

See [“Backing up an embedded database on demand from the Symantec Endpoint Protection Manager”](#) on page 268.

### To back up a site

- 1 In the Symantec Endpoint Protection Manager console, click **Admin**.
- 2 In the Admin page, under Tasks, click **Servers**.
- 3 In the Admin page, under View, click **localhost**.
- 4 In the Admin page, under Tasks, click **Edit Backup Settings**.

- 5 In the Backup Site for Local Site: *Site name of local site* dialog box, select the name of the backup server from the Backup server list.  
  
By default, the pathname is Program Files\Symantec\Symantec Endpoint Protection Manager\data\backup.  
  
However, you can change the name of the backup path by using one of the available backup utilities.
- 6 Select the number of backups that you want to retain from the Number of backups to keep list.  
  
You can select up to 10 backups that you can retain before a backup copy is automatically deleted.
- 7 Click **OK**.

## Deleting remote sites

When you remove a server at a company's remote site, you need to manually delete it from all Symantec Endpoint Protection Manager consoles. The servers are listed under Remote Sites. Uninstalling the software from one Symantec Endpoint Protection Manager console does not make the icon disappear from the Servers pane on other Symantec Endpoint Protection Manager consoles.

### To delete remote sites

- 1 In the Symantec Endpoint Protection Manager console, click **Admin**.
- 2 In the Admin page, under Tasks, click **Servers**.
- 3 In the Admin page, under View, click **Remote Sites**.
- 4 In the Admin page, under View, expand Remote Sites and select the site that you plan to delete.
- 5 Click **Delete Remote Site**.

In the Delete Remote Site dialog, you are prompted to confirm the deletion of the remote site:

```
Deleting remote site also removes all the
replication partnerships in which this site participates.
```

```
Are you sure you want to delete this site?
```

- 6 Click **Yes** to delete the remote site.  
  
You can add back a remote site that was deleted by adding a replication partner.

# Managing servers

This chapter includes the following topics:

- [About the management of servers](#)
- [About servers and third-party passwords](#)
- [Starting and stopping the Symantec Endpoint Protection Manager service](#)
- [Granting or denying access to remote Symantec Endpoint Protection Manager consoles](#)
- [Deleting selected servers](#)
- [Exporting and importing server settings](#)

## About the management of servers

You can centrally manage all types of servers from the Admin page in the Symantec Endpoint Protection Manager console.

The Admin page, under View Servers, lists the following groupings:

- **Local Site**  
The Symantec Endpoint Protection Manager console on the local site, databases, replication partners, such as other Symantec Endpoint Protection Manager consoles whose databases replicate, and optional Enforcers
- **Remote Sites**  
The Symantec Endpoint Protection Manager console on any remote site, databases, replication partners, such as other Symantec Endpoint Protection Managers whose databases replicate, and optional Enforcers

## About servers and third-party passwords

All of the servers for which you can establish a connection require you to configure third-party passwords in Symantec Endpoint Protection Manager. The third-party passwords are automatically saved in the database that you created when you initially installed Symantec Endpoint Protection Manager.

You are typically prompted to provide the third-party password during the configuration of the following types of servers:

- Email servers
- Directory servers
- RSA servers
- Proxy servers

## Starting and stopping the Symantec Endpoint Protection Manager service

When you install the Symantec Endpoint Protection Manager, the last step of the Server Configuration Assistant includes a Symantec Endpoint Protection Manager console check box (selected by default). If you leave the check box selected, the Symantec Endpoint Protection Manager console automatically starts.

The Symantec Endpoint Protection Manager runs as an automatic service. If it did not start automatically, you can start it (and later stop it) by using Services from the Administrative Tools from the Start menu.

From a command prompt, you can start and stop the Symantec Endpoint Protection Manager service as follows:

```
net start Symantec Endpoint Protection Manager consolesemsrv
```

and

```
net stop semsrv
```

You can also restart the Symantec Endpoint Protection Manager console to start the service automatically.

---

**Note:** If you stop the Symantec Endpoint Protection Manager service, clients can no longer connect to it. If clients are required to communicate with the Symantec Endpoint Protection Manager to connect to the network, they are denied access until the Symantec Endpoint Protection Manager service is restarted.

For example, a client must communicate with the Symantec Endpoint Protection Manager to pass a Host Integrity check.

---

## Granting or denying access to remote Symantec Endpoint Protection Manager consoles

You can secure the main Symantec Endpoint Protection Manager console by granting or denying access to those computers on which a remote Symantec Endpoint Protection Manager console is installed. By default, all consoles are allowed access. Administrators can log on to the main Symantec Endpoint Protection Manager console locally or remotely from any computer on the network.

In addition to globally granting or denying access, you can specify exceptions by IP address. The exception list automatically denies access if you have chosen to grant access to all remote consoles. Conversely, if you deny access to all remote consoles, you automatically grant access to all exceptions.

When you create an exception, the computer that you specified must have a static IP address. You can also create an exception for a group of computers by specifying a subnet mask. For example, you may want to allow access in all areas that you administer. However, you may want to deny access to a Symantec Endpoint Protection Manager console that is located in a public area.

### To grant or deny access to a remote Symantec Endpoint Protection Manager console

- 1 In the Symantec Endpoint Protection Manager console, click **Admin**.
- 2 In the Admin page, under Tasks, click **Servers**.
- 3 In the Admin page, under View Servers, select the server whose console access permission you want to change.
- 4 Under Tasks, click **Edit Server Properties**.
- 5 In the General tab, click **Granted Access** or **Denied Access**.
- 6 If you want to specify IP addresses of the computers that are exempt from this console access permission, click **Add**.

Computers that you add become exceptions to those that are granted access. Access is denied to these computers. If you select Denied Access, the computers that you specify become the only ones that are allowed access. Create an exception for a single computer or a group of computers.

- 7 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.
- 8 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.
- 9 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.
- 10 Click **OK**.
- 11 When you finish adding exceptions to the list or editing the list, click **OK**.

## Deleting selected servers

You may have uninstalled multiple installations of Symantec Endpoint Protection Manager. However, they might still display in the Symantec Endpoint Protection Manager console. In this situation, you must delete the connections.

The most common occurrence of this situation is when you use a Microsoft SQL database with multiple Symantec Endpoint Protection Managers connected to it. If one Symantec Endpoint Protection Manager is uninstalled, it still appears on the other Symantec Endpoint Protection Manager consoles. You need to manually delete the servers that are no longer connected.

### To delete selected servers

- 1 In the Symantec Endpoint Protection Manager console, click **Admin**.
- 2 In the Admin page, under Tasks, click **Servers**.



- 3 In the Admin page, under View Servers, expand Local Site (Site <sitename>) to select the Symantec Endpoint Protection Manager that you want to delete.

Note that you must stop the Symantec Endpoint Protection Manager service before you can delete it.

See [“Starting and stopping the Symantec Endpoint Protection Manager service”](#) on page 230.

- 4 Click **Delete Selected Server**.
- 5 Click **Yes** to verify that you want to delete the selected server.

## Exporting and importing server settings

You may want to export or import settings for a Symantec Endpoint Protection Manager. Settings are exported to a file in xml format.

### To export server settings

- 1 Click the **Servers** tab.
- 2 In the tree, expand Local Site (Site *sitename*), 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 Click the **Servers** tab.
- 2 In the tree, expand Local Site (Site *sitename*), and then select the management server for which you want to import settings.
- 3 Click **Import Server Properties**.
- 4 Select the file you want to import, and then click **Import**.
- 5 Click **Yes** to confirm the import.



# Managing directory servers

This chapter includes the following topics:

- [About the management of directory servers](#)
- [Adding directory servers](#)
- [Synchronizing user accounts between directory servers and a Symantec Endpoint Protection Manager](#)
- [Importing information about users from an LDAP directory server](#)
- [Searching for users on an LDAP directory server](#)
- [Importing users from an LDAP directory server search results list](#)
- [About organizational units and the LDAP server](#)

## About the management of directory servers

You need to configure the Symantec Endpoint Protection Manager to communicate with any directory server. You need to establish a connection between the directory servers and the Symantec Endpoint Protection Manager. If you do not establish a connection, you cannot import users from an Active Directory or LDAP directory servers or synchronize with them.

## Adding directory servers

With Active Directory servers, you cannot filter the users. With LDAP servers, you can filter the users before importing data. Therefore you may want to add an Active Directory server that has LDAP compatibility as an LDAP server if you need to filter the data.

After you complete adding a directory server, you may want to set up synchronization.

See [“Synchronizing user accounts between directory servers and a Symantec Endpoint Protection Manager”](#) on page 237.

#### To add directory servers

- 1 In the Symantec Endpoint Protection Manager console, click **Admin**.
- 2 In the Admin page, under Tasks, click **Servers**.
- 3 In the Admin page, under View Servers, select the Symantec Endpoint Protection Manager to which you want to add a directory server.
- 4 In the Admin page, under Tasks, click **Edit Server Properties**.
- 5 In the Server Properties for *name of site* dialog box, on the Directory Servers tab, click **Add**.
- 6 In the Add Directory Server dialog, type the name for the directory server that you want to add in the Name field.
- 7 In the Add Directory Server dialog, check **Active Directory** or **LDAP** as the Server Type.  
  
You must type the IP address, host name, or domain name of the directory server that you want to add.
- 9 If you add an LDAP server, type the port number of the LDAP server in the LDAP Port box.  
  
You cannot change the values if you add an Active Directory server.  
  
The default port setting is 389.
- 10 If you add an LDAP server, type the LDAP BaseDN in the LDAP BaseDN box.
- 11 Type the user name of the authorized directory server account in the User Name box.
- 12 Type the password for the directory server account in the Password box.
- 13 If you want to connect with the directory server using Secure Sockets Layer (SSL), check **Use Secure Connection**.  
  
If you do not check this option, a normal unencrypted connection is used.
- 14 Click **OK**.

# Synchronizing user accounts between directory servers and a Symantec Endpoint Protection Manager

You can configure directory servers to import and synchronize users with the Symantec Endpoint Protection Manager. You must have already added the directory servers before you can synchronize the information about users.

## To synchronize user accounts between directory servers and a Symantec Endpoint Protection Manager

- 1 In the Symantec Endpoint Protection Manager console, click **Admin**.
- 2 In the Admin page, under Tasks, click **Servers**.
- 3 In the Admin page, under View, select the Symantec Endpoint Protection Manager to which you want to add a directory server.
- 4 In the Admin page, under Tasks, click **Edit Server Properties**.
- 5 In the Server Properties dialog box, click the Directory Servers tab.
- 6 Check **Synchronize with Directory Servers** if not already checked.  
This option is the default setting.
- 7 To set up the schedule for how often you want to synchronize the management server with the directory server, do one of the following actions:
  - To synchronize automatically every 24 hours, click **Auto-schedule**.  
The default setting is scheduled to synchronize every 86400 seconds. You can also customize the interval by editing the `tomcat\etc\conf.properties` file.
  - To specify how often you want to synchronize, click **Synchronize every** and specify the number of hours.
- 8 Click **OK**.

## Importing information about users from an LDAP directory server

Administrators can import information about user and computer accounts from an LDAP directory server by using the LDAP protocol.

If you plan to import information about user and accounts, you must first establish a connection between the Symantec Endpoint Protection Manager and a directory server.

See [“Adding directory servers”](#) on page 235.

You can then search for and import information about users and accounts by completing the following tasks:

- Search the LDAP server for users.  
See [“Searching for users on an LDAP directory server”](#) on page 238.
- Import the information about the user accounts.  
See [“Importing users from an LDAP directory server search results list”](#) on page 240.

## Searching for users on an LDAP directory server

You need to search for users on an LDAP server when you import information about users to the management server.

### To search for users on an LDAP directory server

- 1 In the Symantec Endpoint Protection Manager console, click **Clients**.
- 2 In the Clients page, under View, select the group into which you want to import users.
- 3 In the Clients page, under Tasks, click **Import Active Directory or LDAP Users**.
- 4 In the Import Active Directory or LDAP Users dialog box, type the IP address or host name in the Server box.
- 5 In the Import Active Directory or LDAP Users dialog box, type the port number of the LDAP server or Active Directory server in the Server Port box.  
The default port number is 389.
- 6 If you want to connect with the directory server using Secure Sockets Layer (SSL), click **Use Secure Connection**.

If you do not check this option, an unencrypted connection is used.

**7 List the users by clicking **List Users**.**

You can also type an LDAP query to locate the names of users that you want to import in the LDAP Search Base box.

You can specify search options such as attribute=value pairs. Commas must separate the attributes.

CN	CommonName
DC	DomainComponent
L	LocalityName
ST	StateOrProvinceName
O	OrganizationName
OU	OrganizationalUnitName
C	CountryName
STREET	StreetAddress

Not all LDAP servers support all options. For example, Microsoft Active Directory does not support O.

The order in which you specify the attribute=value pairs is important because it indicates the location of the entry in the LDAP directory hierarchy.

If during the installation of a directory server, you specified a DNS-type domain name such as itsupport.sygate.com, you can query a directory server, as itsupport is a typical NT NetBIOS domain name.

To query that Active Directory server, specify the LDAP search base in this order:

```
CN=Users, DC=itsupport, DC=sygate, DC=com
```

You can use wild-card characters or regular expressions in the search base. For example:

```
CN=a*, CN=Users, DC=itsupport, DC=sygate, DC=com
```

This query returns all the user names that start with the letter a.

Another example represents organizations in which you may want to perform a structural directory search, such as:

```
mycorp.com -> engineering.mycorp.com or sales.mycorp.com
```

You can specify either option contingent upon where you want to start searching the LDAP directory.

`o=mycorp.com` or `o=engineering.mycorp.com`

You can specify logical comparison using `>` or `<` in an LDAP search string.

An LDAP query that provides more than 1,000 results may fail. Be sure to set up the search base so that fewer than 1,000 users are reported.

- 8 Type the name of the LDAP user account in the Authorized Accounts box.
- 9 Type the password of the LDAP user account in the Password box.
- 10 Click **List Users** to display a list of users on the LDAP server.

If Only show users that are not added in any group is checked, only those users appear that have not already been added.

## Importing users from an LDAP directory server search results list

You can also import users from an LDAP server search results list.

### To import users from an LDAP directory server search results list

- 1 In the Symantec Endpoint Protection Manager console, click **Clients**.
- 2 In the Group List tree, select the group to which you want to add users from the LDAP server.

Click **Add All** if you want to add all users or select specific users from the list, and then click **Add**.

- 3 Click the field name to sort by using that column.

You can sort the search results by field in ascending or descending order.

- 4 Select one or more users from the LDAP User List area.

You can use standard windows selection keys such as the Ctrl key to select non-contiguous users.

- 5 Click **Add** so that the names of new users appear in the group tree.
- 6 Repeat this process for adding users to other groups, as necessary, until you have added all new users to appropriate groups.
- 7 Click **Close**.



## About organizational units and the LDAP server

The Symantec Endpoint Protection Manager can automatically synchronize users, computers, and the entire group structure in an organizational unit (OU) from an Active Directory or LDAP server. When imported, you can assign policies to the groups that are created. Imported organizational units cannot be modified in the Symantec Endpoint Protection Manager console. If you need to add, delete, or modify them in any way, you must perform these tasks on the LDAP server. The Symantec Endpoint Protection Manager automatically remains synchronized with the structure that is implemented on the directory server if you enable synchronization.

You can also create groups on the Symantec Endpoint Protection Manager and copy users into them from the OUs. The same user may exist in both the group on the management server and an OU. In this situation, the priority of the group is higher than the priority of the OU. Therefore the policy of the group applies to the user or computer.

### Importing organizational units from an active or LDAP directory server

If you want to import an organizational unit or container, you must have already connected a Symantec Endpoint Protection Manager to an LDAP server.

See [“Adding directory servers”](#) on page 235.

You cannot filter any results from the Import Organizational Units dialog box. If you need to filter users, you must do so when you add the LDAP server to the Symantec Endpoint Protection Manager. Active Directory servers cannot be filtered in either place.

This process may take time, depending on the number of users. An organizational unit cannot be placed in more than one group tree.

#### To import an organizational unit from an LDAP server

- 1 In the Symantec Endpoint Protection Manager console, click **Clients**.
- 2 In the Clients page, under View, select the group to which you want to add the organizational unit or Container.
- 3 In the Clients page, under Tasks, click **Import Organizational Unit or Container**.
- 4 Choose the domain.
- 5 Select the organizational unit.
- 6 Click **OK**.

## Synchronizing organizational units

Integration and synchronization with LDAP servers and Active Directory is an optional feature of the Symantec Endpoint Protection Manager. You can import organizational units from other servers and set up automatic synchronization of the imported OUs with the other servers.

Any changes that you made on the LDAP server do not appear immediately in the organizational unit that was imported into the Symantec Endpoint Protection Manager. The latency period is dependent on the synchronization frequency. You can set the synchronization frequency by editing server properties on the Symantec Endpoint Protection Manager.

The name of the user still appears in the group on the Symantec Endpoint Protection Manager even if you had performed the following tasks:

- Copied a user from an organizational unit to a group
- Deleted that user from the LDAP server subsequently

The synchronization occurs only between the LDAP server and the organizational unit.

# Managing email servers

This chapter includes the following topics:

- [About managing email servers](#)
- [Establishing communication between Symantec Endpoint Protection Manager and email servers](#)

## About managing email servers

If your network supports email servers, you may want to perform the following tasks after you establish communication between the Symantec Endpoint Protection Manager and the email server:

- Set up automatic email notifications for security events to be sent to administrators
- Set up automatic email notifications for security events to be sent to clients

Automatic email notifications can occur only if you establish a connection between Symantec Endpoint Protection Manager and at least one of the email servers in the network.

See [“Configuring email messages for traffic events”](#) on page 476.

## Establishing communication between Symantec Endpoint Protection Manager and email servers

If you want to use email notification, you need to configure the email server on the Symantec Endpoint Protection Manager.

**To establish communication between Symantec Endpoint Protection Manager and email servers**

- 1** In the Symantec Endpoint Protection Manager console, click **Admin**.
- 2** In the Admin page, under Tasks, click **Server**.
- 3** In the Admin page, under View Servers, select the Symantec Endpoint Protection Manager for which you want to establish a connection to the email server.
- 4** In the Admin page, under Tasks, click **Edit Server Properties**.
- 5** In the Server Properties dialog box, click the **Mail Server** tab.
- 6** Type the IP address, host name, or domain name of the email server in the Server Address text box.
- 7** Type the user name of the account on the email server in the User Name text box.  
  
You need to add a user name only if the email server requires authentication.
- 8** In the Server Properties dialog box, type the password of an account on the email server in the Password text box.  
  
You need to add a password only if the email server requires authentication
- 9** Click **OK**.

# Managing proxy servers

This chapter includes the following topics:

- [About proxy servers](#)
- [Setting up a connection between an HTTP proxy server and the Symantec Endpoint Protection Manager](#)
- [Setting up a connection between an FTP proxy server and the Symantec Endpoint Protection Manager](#)

## About proxy servers

You can use HTTP proxy and FTP proxy servers to help you manage LiveUpdates.

You can establish connections between the Symantec Endpoint Protection Manager and the following server types:

- HTTP proxy server
- FTP proxy server

## Setting up a connection between an HTTP proxy server and the Symantec Endpoint Protection Manager

If you support an HTTP proxy server in the corporate network, you need to connect the HTTP proxy server to the Symantec Endpoint Protection Manager. You can use the HTTP proxy server to automatically download LiveUpdate contents.

**To set up an HTTP proxy server**

- 1 In the Symantec Endpoint Protection Manager console, click **Admin**.
- 2 In the Admin page, under Tasks, click **Servers**.
- 3 Under View Servers, select the Symantec Endpoint Protection Manager to which you want to connect an HTTP proxy server.
- 4 Under Tasks, click **Edit Server Properties**.
- 5 In the Server Properties dialog, click the **Proxy Server** tab.
- 6 Under HTTP proxy settings, select **Use custom proxy settings** from the Proxy usage list.
- 7 Type the IP address of the HTTP proxy server in the Server address field.  
A valid IP address or server name of up to 256 characters.
- 8 Type the port number of the proxy server in the Port field.  
A valid port number ranges from 0 - 65535.
- 9 Check **Authentication needed to connect through proxy server**.
- 10 Type the user name of the proxy server in the User name field.
- 11 Type the password of the proxy server to which you want to connect in the Password field.
- 12 Click **OK**.

## Setting up a connection between an FTP proxy server and the Symantec Endpoint Protection Manager

If you support an FTP proxy server in the corporate network, you need to connect the FTP proxy server to the Symantec Endpoint Protection Manager. You can use the HTTP proxy server to automatically download LiveUpdate contents.

**To set up a connection between an FTP proxy server and the Symantec Endpoint Protection Manager**

- 1 In the Symantec Endpoint Protection Manager console, click **Admin**.
- 2 In the Admin page, under Tasks, click **Servers**.
- 3 Under View Servers, select the Symantec Endpoint Protection Manager to which you want to connect an FTP proxy server.
- 4 Under Tasks, click **Edit Server Properties**.
- 5 In the Server Properties dialog, click the **Proxy Server** tab.

**Setting up a connection between an FTP proxy server and the Symantec Endpoint Protection Manager**

- 6** Under FTP proxy settings, select **Use custom proxy settings** from the Proxy usage list.
- 7** Type the IP address of the FTP proxy server in the Server address field.  
The IP address or server name can contain up to 256 characters.
- 8** Type the port number of the proxy server in the Port field.  
A valid port number ranges from 0 - 65535.
- 9** Click **OK**.





# Managing RSA servers

This chapter includes the following topics:

- [About prerequisites for using RSA SecurID with the Symantec Endpoint Protection Manager](#)
- [Configuring the Symantec Endpoint Protection Manager to use RSA SecurID Authentication](#)
- [Specifying SecurID Authentication for a Symantec Endpoint Protection Manager administrator](#)
- [Configuring the management server to support HTTPS communication](#)

## About prerequisites for using RSA SecurID with the Symantec Endpoint Protection Manager

If you want to authenticate administrators that use the Symantec Endpoint Protection Manager with RSA SecurID, you need to enable encrypted authentication by running the RSA installation wizard.

Before you run the wizard, make sure that:

- You have an RSA ACE server installed
- The computer on which you installed the Symantec Endpoint Protection Manager is registered as a valid host on the RSA ACE server
- Create the Node Secret file for the same host
- The `sdconf.rec` file on the RSA ACE server is accessible on the network
- A synchronized SecurID card or key fob has been assigned to a Symantec Endpoint Protection Manager account. The logon name must be activated on the RSA ACE server

- The administrator has the RSA PIN or password available

Symantec supports the following types of RSA logons:

- RSA SecurID token (not software RSA tokens)
- RSA SecurID card
- RSA keypad card (not RSA smart cards)

To log on to the Symantec Endpoint Protection Manager with the RSA SecurID, the administrator needs a logon name, the token (hardware), and a pin number.

## Configuring the Symantec Endpoint Protection Manager to use RSA SecurID Authentication

If your corporate network includes an RSA server, you need to install the software for an RSA ACE Agent on the computer on which you installed the Symantec Endpoint Protection Manager and configure it as a SecurID Authentication client. The Symantec Endpoint Protection Manager is also referred to as the management server.

### To configure RSA SecurID authentication on the Symantec Endpoint Protection Manager

- 1 Install the software for the RSA ACE Agent on the same computer on which you installed the Symantec Endpoint Protection Manager. You can install the software by running the Windows .msi file from the RSA Authentication Agent CD.
- 2 Copy the `nodesecret.rec`, `sdconf.rec`, and `agent_nsload.exe` files from the RSA ACE server to the computer on which you installed the Symantec Endpoint Protection Manager.
- 3 At the command prompt, type the following command:  

```
agent_nsload -f nodesecret.rec -p password for the nodesecret file
```
- 4 In the management console, click **Admin**.
- 5 In the Admin page, under Tasks, click **Servers**.
- 6 In the Admin page, under View Servers, select the Symantec Endpoint Protection Manager to which you want to connect an RSA server.
- 7 In the Admin page, under Tasks, click **Configure SecurID authentication**.
- 8 In the Welcome to the Configure SecurID Authentication Wizard panel, click **Next**.

## Specifying SecurID Authentication for a Symantec Endpoint Protection Manager administrator

- 9 In the Qualification panel of the Configure SecurID Authentication Wizard panel, read the prerequisites so that you can meet all the requirements.
- 10 Click **Next**.
- 11 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.
- 12 Click **Next**.
- 13 Click **Test** to test your configuration.
- 14 In the Test Configuration dialog box, type the user name and password for your SecurID, and then click **Test**.  
It now authenticates successfully.

## Specifying SecurID Authentication for a Symantec Endpoint Protection Manager administrator

You can specify that administrators must first be authenticated by SecurID before they can log into the management console.

You can create a new administrator or modify the settings for an existing administrator. The procedure here describes how to specify the authentication for a new administrator.

See [“Adding an administrator”](#) on page 69.

### To create a SecurID authentication for a Symantec Endpoint Protection Manager administrator

- 1 In the management console, click **Admin**.
- 2 On the Admin page, under Tasks, select **Administrators**.
- 3 On the Administrators page, under Tasks, select **Add Administrator**.
- 4 In the Add Administrator dialog box, type the name of a user that you previously configured for the RSA ACE client.
- 5 Next to Authentication Type, click **Change**.
- 6 In the Administrator Authentication dialog box, select **RSA SecurID Authentication**, and then click **OK**.
- 7 In the Add Administrator dialog box, click **OK**.

## Configuring the management server to support HTTPS communication

If you plan to use HTTPS communication and SSL authentication between clients, Symantec Endpoint Protection Managers, and optional Enforcers, you need to add an SSL certificate. You need to add the SSL certificate to Microsoft's Internet Information Server (IIS).

You need to complete the following tasks, in this order:

- Generate or purchase an SSL certificate.
- Add the certificate to the IIS server that is installed on the same computer as the Symantec Endpoint Protection Manager.
- Configure the management server lists to support HTTPS communication.

### To add the certificate to the IIS server

- 1 Click **Start > Programs > Administrative Tools > Internet Information Services (IIS) Manager**.
- 2 Under the local computer, select Symantec Web Server under Web Sites.
- 3 Right-click **Symantec Web Server**, and choose Properties.
- 4 On the Directory Security tab, click **Server Certificate** to start the Web Server Certificate Wizard.
- 5 Create or import a server certificate by following the steps in the wizard.  
For more information, see the IIS online Help.
- 6 On the Web Site tab, specify the port number for the SSL port, which is 443 by default.

# Managing server certificates

This chapter includes the following topics:

- [About server certificate types](#)
- [Updating a server certificate with a wizard](#)
- [Backing up a server certificate](#)
- [Locating the keystore password](#)

## About server certificate types

Digital certificates are the industry standard for authenticating and encrypting sensitive data. If you want to prevent the reading of information as it passes through routers in the network, you need to encrypt the data. Therefore you need a digital certificate that uses the HTTPS protocol.

As part of this secure procedure, the server identifies and authenticates itself with a server certificate. Symantec uses the HTTPS protocol for the communication between all the servers, clients, and optional Enforcers in a network.

You must also enable encryption on the management server so that the server identifies and authenticates itself with a server certificate. If you do not enable this option, then the installation of a digital certificate is not effective.

The Symantec Endpoint Protection Manager supports the following types of certificate:

- JKS keystore file (.jks)  
A Java tool that is called `keytool.exe` generates the keystore file. Symantec supports only the Java Key Standard (JKS) format. The Java Cryptography

Extension (JCEKS) format requires a specific version of the Java Runtime Environment (JRE). The Symantec Endpoint Protection Manager supports only a JCEKS keystore file that is generated with the same version as the Java Development Kit (JDK) on the Symantec Endpoint Protection Manager.

- PKCS12 keystore file (.pfx and .p12)  
The keystore must contain both a certificate and a private key. The keystore password must be the same as the key password. It is usually exported from Internet Information Services (IIS).
- Certificate and private key file (DER and PEM format)  
Symantec supports unencrypted certificates and private keys in the DER or the PEM format. PKCS8-encrypted private key files are not supported.

You may want to back up the information about the certificate as a safety precaution. If the management server is damaged or you forget the keystore password, you can easily retrieve the password.

## Updating a server certificate with a wizard

You can use the Update Server Certificate Wizard to guide you through the process of updating certificates.

### To update a server certificate with a wizard

- 1 In the Symantec Endpoint Protection Manager console, click **Admin**.
- 2 In the Admin page, under Tasks, click **Servers**.
- 3 Under View Servers, click the management server for which you want to update the server certificate.
- 4 Under Tasks, click **Manage Server Certificate**.
- 5 In the Welcome to the Manage Server Certificate Wizard pane, click **Next**.
- 6 In the Manage Server Certificate pane, click **Update the server certificate**.

- 7 In the Manage Server Certificate pane, click **Next**.
- 8 Select any of the following options to install or update a server certificate:

JKS keystore file (.jks)	See <a href="#">“Updating a JKS certificate with a wizard”</a> on page 255.
PKCS12 keystore file (.pfx and .p12)	See <a href="#">“Updating a PKCS12 certificate with a wizard”</a> on page 255.
Certificate and private key file (DER and PEM format)	See <a href="#">“Updating unencrypted certificates and private keys (DER or PEM) with a wizard”</a> on page 256.

### Updating a JKS certificate with a wizard

- 1 Complete steps 1 through 8 unless you have already done so.
- 2 In the Update Server Certificate panel, click **JKS keystore file (.jks)**.
- 3 Click **Next**.
- 4 In the JKS Keystore panel, click **Browse** to locate the JKS keystore file (.jks) on the management server, or type the pathname for this file in the text field.
- 5 In the Select Java Keystore File dialog box, click **Open** after you have located the file.
- 6 In the JKS Keystore panel, type the Keystore password into the Keystore password text box.
- 7 In the JKS Keystore panel, type the Keystore password into the Key password text field for the second time.
- 8 In the JKS Keystore panel, click **Next**.
- 9 In the Manage Server Certificate Wizard is complete panel, click **Finish**.

In the Manage Server Certificate Wizard is complete panel, a message appears that states whether or not the server certificates was successfully added. You need to log off and restart the management server before the certificate becomes effective.

### Updating a PKCS12 certificate with a wizard

- 1 Complete steps 1 through 8 unless you have already done so.
- 2 In the Update Server Certificate panel, click **PKCS12 keystore file (.pfx and .p12)**.
- 3 Click **Next**.

- 4 In the PKCS12 Keystore panel, click **Browse** to locate the PKCS12 keystore file (.pfx and .p12) on the management server, or type the pathname for this file in the text field.
- 5 In the Select PKCS12 File dialog box, click **Open** after you have located the file.
- 6 In the PKCS12 Keystore panel, type the Keystore password into the Keystore password text box.
- 7 In the PKCS12 Keystore panel, click **Next**.
- 8 In the Manage Server Certificate Wizard is complete panel, click **Finish**.

In the Manage Server Certificate Wizard is complete panel, a message appears that states whether or not the server certificates was successfully added. You need to log off and restart the management server before the certificate becomes effective.

#### **Updating unencrypted certificates and private keys (DER or PEM) with a wizard**

- 1 Complete steps 1 through 8 unless you have already done so.
- 2 In the Update Server Certificate panel, click **Certificate and private key file (DER and PEM format)**.
- 3 Click **Next**.
- 4 In the Certificate File panel, locate the certificate (DER and PEM format) on the management server by clicking **Browse**.  
  
Alternately, type the pathname for this file in the Certificate path text box.
- 5 In the Certificate File panel, click **Browse** to locate the private key file (DER and PEM format) on the management server. Alternately, type the pathname for this file in the Private key file text box.
- 6 In the Certificate File panel, click **Next** after you have located the files.
- 7 In the Manage Server Certificate Wizard is complete panel, click **Finish**.

In the Manage Server Certificate Wizard is complete panel, a message appears that states whether or not the server certificates was successfully added. You need to log off and restart the management server before the certificate becomes effective.

## **Backing up a server certificate**

In case the management server is damaged, you must back up the private key as well as the files that represent the certificate.



**To back up a server certificate**

- 1 In the Symantec Endpoint Protection Manager console, click **Admin**.
- 2 In the Admin page, under Tasks, click **Servers**.
- 3 Under View Servers, click the management server whose server certificate you want to back up.
- 4 Under Tasks, click **Manage Server Certificate**.
- 5 In the Welcome to the Manage Server Certificate Wizard pane, click **Next**.
- 6 In the Manage Server Certificate panel, click **Back up the server certificate**.
- 7 In the Backup Server Certificate panel, type the pathname or browse to the folder into which you want to back up the private key. Note that you back up the management server certificate into the same folder.

The JKS Keystore file is backed up during the initial installation. A file that is called *servertimestamp.xml* is also backed up. The JKS Keystore file includes the server's private and public key pair and the self-signed certificate.

- 8 In the Backup Server Certificate panel, click **Next**.
- 9 In the Manage Server Certificate panel, click **Finish**.

## Locating the keystore password

You may need to locate the password in case you misplaced it.

**To locate the keyword password**

- 1 Right-click **My Computer**.
- 2 Locate the folder into which you backed up the files for the certificate by selecting **Explorer**.
- 3 Open the *servertimestamp.xml* file and locate the keystore password.
- 4 Paste the keystore password into the Keystore and Key password fields.



# Managing databases

This chapter includes the following topics:

- [About the management of databases](#)
- [Backing up a Microsoft SQL database](#)
- [Backing up an embedded database on demand from the Symantec Endpoint Protection Manager](#)
- [Scheduling automatic database backups from the Symantec Endpoint Protection Manager](#)
- [Restoring a database](#)
- [Editing the name and description of a database in the Symantec Endpoint Protection Manager console](#)
- [Reconfiguring a database](#)
- [About managing log data](#)

## About the management of databases

Symantec Endpoint Protection and Symantec Network Access Control support a Microsoft SQL or an embedded database. The embedded database is typically used for organizations with 1000 or fewer clients that connect to the Symantec Endpoint Protection Manager console. Larger organizations typically use Microsoft SQL Server for the database.

If you install an embedded database, Symantec Endpoint Protection Manager can automatically install the database. Should your company environment already support an MS SQL server, then you may want to take advantage of the existing hardware and software. MS SQL servers typically allow you to support a larger number of clients.

A database contains information about security and enforcement policies. In addition, all configuration settings, data about attacks, logs, and reports are also included in the database. Therefore you can monitor security breaches on the network.

The information in the database is stored in tables, also called a database schema. The schema is provided for administrators who may need it for specialized reporting.

## About the naming conventions of a database

A Microsoft SQL database uses different naming conventions than an embedded database.

### Naming convention for a Microsoft SQL database

You can install a Microsoft SQL database on the same computer as the Symantec Endpoint Protection Manager or on a separate one. In both cases the Microsoft SQL database keeps the same name as the computer on which the Microsoft SQL database server is installed.

You can install the management server and the Microsoft SQL database on the same computer that is called PolicyMgrCorp. The database retains the same name as the computer on which it is installed. The database name appears in the tree of the Admin page under View. It also appears as the Database Address of the Microsoft SQL database in the Database Management pane.

### Naming convention for an embedded database

If you use an embedded database, the name of the database is always called localhost.

The name, localhost, appears in the Admin page under View. It is also listed as the Database Address of the embedded database in the Database Management pane.

## Management Server Configuration Wizard and Symantec Database Tools

You can back up, schedule, and edit certain database settings, such as the name of a database, from the Symantec Endpoint Protection Manager console. However, you can only restore and reconfigure databases by using the Management Server Configuration Wizard and the Symantec Database Backup and Restore utility.

You can use the Management Server Configuration Wizard to reconfigure all of the MS SQL and embedded database settings.

See [“About the reconfiguration of a database”](#) on page 262.

You can use the Symantec Database Tools utility to back up, restore, and reconfigure all of the MS SQL and embedded database settings.

See [“About the backup and restoration of a database”](#) on page 261.

## About the backup and restoration of a database

Because the size of a database increases over time, you need to regularly back up the database. If a disaster occurs, you need to restore the latest snapshot of the database. Backing up databases and removing unused space from databases is a necessary step in the maintenance of a production database.

### Database backups

When you back up a database, you create a separate copy of the database. In case of data corruption or hardware failure, you can revert to a previous backup. If you want to get a clean copy of the database, you must revert to the point before the problem occurred. Some data may need to be reentered into the database during the recovery process. However, the main structure and a majority of the data is retained by using a recent backup. You can back up the database from the Symantec Endpoint Protection Manager console or by using the Symantec Database Backup and Restore utility. The Symantec Database Backup and Restore utility is automatically installed during the installation.

You can back up in the following ways:

- Microsoft SQL database only  
You can use the Microsoft SQL Server Enterprise Manager to set up a maintenance plan that includes automatic backups.
- Embedded or a Microsoft SQL database  
You can perform an on-demand backup and also schedule automatic backups to occur from the Symantec Endpoint Protection Manager console.

Backups should preferably be stored on a separate disk drive. You should back up the disk drive periodically.

See [“Backing up a Microsoft SQL database”](#) on page 263.

See [“Backing up an embedded database on demand from the Symantec Endpoint Protection Manager”](#) on page 268.

### Database restoration

You may need to restore a database for a number of reasons.

Restoration of a database must occur in the following cases:

- The data in the database becomes corrupted.
- The hardware failed.

You want to convert an embedded database to a Microsoft SQL database or vice versa.

If data already exists in the old database, you need to perform the following tasks:

- Back up the site.
- Reconfigure the database.
- Create a new empty database.
- Restore the database.

If you have a backup copy of a database, you can restore that database on the computer on which the Symantec Endpoint Protection Manager was installed. You can also restore the database on any other computer.

You use the Symantec Database Backup and Restore utility to restore a database. This tool is automatically installed when you install the Symantec Endpoint Protection Manager.

See [“Restoring a database”](#) on page 270.

## About the reconfiguration of a database

You need to reconfigure the database in a number of different circumstances:

- The IP address or the host name of the database server was changed.
- The port of the database server through which it connects to the Symantec Endpoint Protection Manager was changed.
- The name of the database was changed.

---

**Note:** You can also change the name of the database in the Symantec Endpoint Protection Manager.

---

See [“Editing the name and description of a database in the Symantec Endpoint Protection Manager console”](#) on page 271.

- MS SQL only: The name of the user who is responsible for the database was changed. If you modify the database server's user name on a database server, the Symantec Endpoint Protection Manager console can no longer connect to the database server.
- The password of the user who is responsible for the database was changed. You can modify the password of the user who is responsible for the database

server. If you modify the password, the management server can no longer connect to the database server.

- MS SQL only: The SQL Client Path was changed. The SQL client bin folder that by default is located in C:\Program Files\Microsoft SQL Server\80\Tools\Binn was changed.

If you changed the SQL Client Path on the Microsoft SQL database server, the Symantec Endpoint Protection Manager console can no longer connect to the database server.

- You upgrade an embedded database to a Microsoft SQL database.

See [“Reconfiguring a database”](#) on page 272.

See the *Installation Guide for Symantec Endpoint Protection and Symantec Network Access Control*. It provides information on how to upgrade from an embedded database to a Microsoft SQL database.

## About the scheduling of a database backup

You can perform on-demand backups of databases or set up a schedule for automatic backups of MS SQL and embedded databases in Symantec Endpoint Protection Manager. However, you can also use the MS SQL Server's Database Maintenance Wizard to schedule automatic backups for a Microsoft SQL database. In addition, you can also use the Symantec Database Backup and Restore utility to back either a Microsoft SQL database or an embedded database.

See [“Scheduling automatic database backups from the Symantec Endpoint Protection Manager”](#) on page 269.

See [“Backing up a Microsoft SQL database on demand from the Symantec Endpoint Protection Manager console”](#) on page 264.

See [“Backing up an embedded database on demand from the Symantec Endpoint Protection Manager”](#) on page 268.

See [“Backing up a Microsoft SQL database with the Database Maintenance Plan wizard”](#) on page 265.

See the *Installation Guide for Symantec Endpoint Protection and Symantec Network Access Control*. It provides information on how to back up a Microsoft SQL database with the Symantec Database Backup and Restore utility.

## Backing up a Microsoft SQL database

You can perform an on-demand backup of a Microsoft SQL database from the Symantec Endpoint Protection Manager console or the Symantec Database Backup and Restore utility. The Symantec Database Backup and Restore utility is

automatically installed during the installation of the Symantec Endpoint Protection Manager. You can also use the Database Maintenance Plan wizard that is included in the MS SQL Server software to back up the Microsoft SQL database. The MS SQL Database Maintenance Plan wizard can also help you set up a backup schedule and other maintenance tasks.

See [“Database backups”](#) on page 261.

See [“Backing up a Microsoft SQL database on demand from the Symantec Endpoint Protection Manager console”](#) on page 264.

See [“Backing up a Microsoft SQL database with the Database Maintenance Plan wizard”](#) on page 265.

See the *Installation Guide for Symantec Endpoint Protection and Symantec Network Access Control*. It provides information on how to back up a Microsoft SQL database with the Symantec Database Backup and Restore utility.

## Backing up a Microsoft SQL database on demand from the Symantec Endpoint Protection Manager console

The Symantec Endpoint Protection Manager console includes a site backup that you can use to back up and later restore the database. In addition, you can set up a maintenance plan on the Microsoft SQL Server Agent.

The following procedure includes recommended settings.

You may need to use different settings depending on the following criteria:

- The size of your organization.
- The amount of disk space you have reserved for backups.
- Any required guidelines at your company.

### To back up a Microsoft SQL database on demand from a Symantec Endpoint Protection Manager console

- 1 In the Symantec Endpoint Protection Manager console, click **Admin**.
- 2 In the Admin page, click **Servers**.
- 3 In the Admin page, under View Servers, click the icon that represents the Microsoft SQL database.
- 4 In the Admin page, under Tasks, click **Backup Site Now**.

This method backs up all of the site data, including the database. You can check the System log as well as the Backup folder for status during and after the backup.

- 5 Click **Close**.



## Backing up a Microsoft SQL database with the Database Maintenance Plan wizard

The Microsoft SQL Server Enterprise Manager provides a wizard to help set up a database maintenance plan. You can use the Database Maintenance Plan wizard to manage the database and to schedule automatic backups of the Microsoft SQL database.

---

**Note:** Make sure that the SQL Server Agent is started.

Sysadmin access rights are required to run the Database Maintenance Plan wizard.

---

Refer to the Microsoft SQL Server documentation for details on how to maintain a Microsoft SQL Server database.

**To back up a Microsoft SQL database by using the Database Maintenance Plan wizard in the Microsoft SQL Server 2000 Enterprise Manager**

- 1 On the SQL Server Enterprise Manager, click **Programs > Microsoft SQL Server > Enterprise Manager**.
- 2 Expand server name where *server name* is the name of the server on which the database is installed.
- 3 Double-click the **Management** folder.  
The SQL Server Agent displays a green arrow on the icon if it is already started. If it is not started, start the SQL Server Service Manager by selecting the SQL Server Agent and then right-clicking and choosing **Start**.
- 4 Expand **Databases**.
- 5 Right-click **sem5** and select **All Tasks > Maintenance Plan**.
- 6 On the Welcome to the Database Maintenance Plan Wizard screen, click **Next**.
- 7 On the Select Databases screen, select **These Databases:** and next to it check **sem5** to back up the database. Then click **Next**.
- 8 On the Update Data Optimization Information screen, select **Remove unused space from database files**.
- 9 In the When it grows beyond: text box, type **1024** or an appropriate maximum size depending on the size of your organization.  
When the database exceeds the specified size, unused space is automatically removed.
- 10 In the Amount of free space to remain after shrink text box, choose **20% of the data space** or another amount that is appropriate for your company needs.

- 11 Data is optimized weekly and an acceptable default is specified. If you want to change the schedule, click **Change**.  
In the Edit Recurring Job Schedule dialog box that appears, specify how often and at what time to remove unused space from the database and then click **OK**.
- 12 When you are done setting up optimization, click **Next**.
- 13 On the Database Integrity Check screen, click **Next** without setting this option because the Symantec Endpoint Protection Manager maintains database integrity.
- 14 In the Specify the Database Backup Plan screen, check **Backup the database as part of the maintenance plan** and **Verify the integrity of the backup when complete**.
- 15 Select the media on which to store the backup.
- 16 Click **Change** to modify the schedule for backup.
- 17 In the Edit Recurring Job Schedule dialog box, after Occurs, click **Daily**.  
Select the frequency with which the database needs to be backed up. Every 1 day is recommended.
- 18 Check **Enable Schedule**.
- 19 Set the time for which you want the backups to occur. You can also choose a start and end date, or No end date if applicable, and click **OK**.
- 20 Click **Next**.
- 21 In the Specify Backup Disk Directory screen, choose a backup directory by clicking **Use the backup default directory** (the path is \MSSQL\BACKUP by default) or **Use this directory**.
- 22 Select the directory into which you want to copy files.  
The directory must be located on the same computer as the database. You need to direct the backup to a separate disk drive.
- 23 Check **Create a subdirectory for each database**.
- 24 Click **Remove files older than** and then specify a time period after which the older backups are automatically removed or deleted.  
Make sure you have sufficient disk space to store backups for the time period specified and click **Next**.

**25** Proceed as follows:

If you selected Automatically maintain the Sem5 database during the configuration of the database server Continue with step **41**.

If the Recovery Model dialog box displays Simple Continue with step **41**.

If the Recovery Model dialog box displays Full Continue with step **26**.

**26** In the Specify the Transaction Log Backup Plan screen, check **Backup the transaction log as part of the maintenance plan**.

**27** Select the media on which to store the backup.

**28** Click **Change** to modify the schedule for backing up the transaction log.

The Edit Recurring Job Schedule dialog box appears.

The maximum size of the transaction log is set to 8 GB, by default. If the transaction log reaches the maximum size, it no longer functions and the database may become corrupted. (You can change the maximum size of the transaction log on the SQL Server Enterprise Manager.)

**29** After Occurs, click **Daily**.

Select the frequency with which the transaction log needs to be backed up. **Every 1 day** is recommended. Be sure to check **Enable Schedule**.

**30** Select the frequency at which you want the backups to occur.

The default option is recommended, Occurs every 4 hours.

**31** Select a start and end date or **No end date**, if applicable and click **OK**.

**32** Click **Next**.

**33** On the Specify Backup Disk Directory screen, select a backup directory by clicking **Use the backup default directory** or **Use this directory**.

The default path is \MSSQL\BACKUP.

**34** Select the directory into which you want to copy files.

**35** Check **Create a subdirectory for each database**.

**36** Click **Remove files older than**:

- 37 Specify a time period after which the older backups are automatically removed or deleted.  
Make sure that you have sufficient disk space to store backups for the time period specified and then click **Next**.
- 38 On the Reports to Generate screen, check **Write report to a text file in directory**.  
Specify the full path and name of the text file where you want the report to be generated.
- 39 Check **Delete text report files older than** and leave this set to 4 weeks.
- 40 Check **Send e-mail report to operator** and specify the system administrator to whom the generated report is then sent through SQL mail. If the email operator is not available, select **New Operator** and then click **Next**.
- 41 In the Maintenance Plan History screen, click **Next**.  
You should use the default settings for Maintenance Plan History unless you need to change them.
- 42 In the Completing the Database Maintenance Plan History screen, type a name for the maintenance plan such as SQL Database Maintenance, and then click **Finish**.
- 43 When the plan is complete, view the message that the plan was created successfully and click **OK**.

## Backing up an embedded database on demand from the Symantec Endpoint Protection Manager

You can perform an on-demand backup of an embedded database from the Symantec Endpoint Protection Manager console.

See [“Database backups”](#) on page 261.

Refer to the *Installation Guide for Symantec Endpoint Protection and Symantec Network Access Control*. It provides information on how to back up an embedded database with the Symantec Database Backup and Restore utility.

**To back up an embedded database from a Symantec Endpoint Protection Manager console**

- 1 In the Symantec Endpoint Protection Manager console, click **Admin**.
- 2 In the Admin page, click **Servers**.
- 3 Under View Servers, click the icon that represents the embedded database.

## Scheduling automatic database backups from the Symantec Endpoint Protection Manager

- 4 Under Tasks, click **Back Up Site Now**.

This method backs up all site data, including the database. You can check the System log as well as the Backup folder for status during and after the backup.

- 5 Click **Yes** when the Back Up message appears.
- 6 Click **Close**.

# Scheduling automatic database backups from the Symantec Endpoint Protection Manager

You can establish schedules for the automatic backup of both MS SQL and embedded databases in the Symantec Endpoint Protection Manager.

See [“About the scheduling of a database backup”](#) on page 263.

### To back up an embedded database from a Symantec Endpoint Protection Manager console

- 1 In the Symantec Endpoint Protection Manager console, click **Admin**.
- 2 In the Admin page, click **Servers**.
- 3 Under View Servers, click the icon that represents the MS SQL or embedded database and whose backup settings you want to change.
- 4 In the Admin page, under Tasks, click **Edit Backup Settings**.
- 5 In the Backup Site for Local Site dialog box, click **Schedule Backups**.
- 6 Specify the backup frequency by selecting **Hourly**, **Daily**, or **Weekly**, and then specifying one of the following options:
  - If you choose **Hourly**, in the Start Time box, specify the number of minutes after the hour that backups should occur.
  - If you choose **Daily**, in the Start Time box, specify the hour and minutes to indicate at what time each day backups should occur.
  - If you choose **Weekly**, in the Start Time box, specify the hour and minutes to indicate the time that backups should occur.

- If you choose **Weekly**, specify the **Day of Week** to indicate the day on which backups should occur.
- 7 Click **OK**.
- At the scheduled time, backups occur automatically and are placed in a .zip file that is labeled with the date on which the backup occurs. The backup file is stored in a backup folder that is created in the path as specified for the server data root.
- For example, a backup file that is created on August 1, 2007 at 9:46 AM is called 2007-Aug-01\_09-46-13-AM.zip.

## Restoring a database

If the database no longer functions correctly, you can restore it provided you previously backed it up.

### To restore a database

- 1 Locate the latest backup file that you have. This file is in .zip format and labeled with the date. The file is stored in a backup folder that was created in the path that was specified for the server data root.
- 2 Set up the computer on which you want to restore the database by using one of the following strategies
  - Using another computer  
If the hardware on the previous computer failed, you need to install the operating system and the Symantec Endpoint Protection Manager on the new computer. Even though you replace the database with new data, you still have to configure a database after you complete the installation.
  - Using the same computer  
If the hardware and the Symantec Endpoint Protection Manager function correctly, you can restore the database on the same computer. If you experience problems, you may want to uninstall the Symantec Endpoint Protection Manager, reinstall it, configure the database, and then restore the data.
- 3 Log off the console.
- 4 Stop the Symantec Endpoint Protection Manager service by selecting **Start > Programs > Administrative Tools > Services**.
- 5 Locate the Symantec Endpoint Protection Manager service and then right-click to select **Stop**.

- 6 Select **Start > Programs > Symantec Endpoint Protection Manager > Database Back Up and Restore**.
- 7 Click **Restore**, and then click **Yes** in the message that appears.
- 8 In the Restoring Database dialog box, select the backup that you want to use from the list.
- 9 Click **OK**.

The restoration of the database takes a few minutes. The length of time it takes to complete the task depends on the size of the database, number of users, replication partners, and other criteria.
- 10 As soon as the restoration of the database is completed, the following message appears:

```
Database has been restored successfully.
```
- 11 Click **Exit**.
- 12 Click **Start > Programs > Symantec Endpoint Protection Manager** if you restored the database on a different computer because you need to delete the old database server. Otherwise you have finished restoring the database.
- 13 Log into the Symantec Endpoint Protection Manager console.
- 14 Click **Admin**.
- 15 Click **Servers**.
- 16 In the Admin page, under Tasks, right-click the old database server and select **Delete**.
- 17 Reconfigure additional criteria, such as user names and password, if necessary. See [“Reconfiguring a Microsoft SQL database”](#) on page 272.

## Editing the name and description of a database in the Symantec Endpoint Protection Manager console

You can edit the name and description of a local or a remote database.

You can also edit the name of the database by using the Management Server Configuration Wizard.

See [“Reconfiguring a Microsoft SQL database”](#) on page 272.

### To edit the name and description of a database

- 1 In the Symantec Endpoint Protection Manager console, click **Admin**.
- 2 In the Admin page, click **Servers**.

- 3 Under View Servers, expand **Local Site**.
- 4 Select the local database or expand **Remote Sites** to select the database of a remote site whose properties you want to edit.
- 5 Under Tasks, click **Edit Database Properties**.
- 6 In the Database Properties dialog box, edit the name of the database in the **Name** field.
- 7 In the Database Properties dialog box, edit the description of the database in the **Description** field.
- 8 Click **OK**.

## Reconfiguring a database

You can reconfigure both an MS SQL as well as an embedded database for any of the following reasons:

- Change of database server's IP address
- Change of database server's host name

## Reconfiguring a Microsoft SQL database

You need to use the Management Server Configuration Wizard to reconfigure the Microsoft SQL database.

See [“About the reconfiguration of a database”](#) on page 262.

### To reconfigure a Microsoft SQL database

- 1 Stop the Symantec Endpoint Protection Manager service by selecting **Start > All Programs > Administrative Tools > Services**.
- 2 Locate the Symantec Endpoint Protection Manager and then right-click to select **Stop**.
- 3 Click **Start > All Programs > Symantec Endpoint Protection Manager > Management Server Configuration Wizard**.
- 4 In the Welcome to the Management Server Configuration Wizard screen, click **Reconfigure the management server**.
- 5 Click **Next** to begin the reconfiguration.
- 6 Edit the name of the computer on which the Symantec Endpoint Protection Manager is installed in the Server name box.



- 7 Edit the HTTPS port number that the Symantec Endpoint Protection Manager listens on in the Server port box.  
 The default port number is 8443.
- 8 Edit the location of the server data folder or browse to the root folder where data files are located.  
 The root folder includes backups, replication, and other Symantec Endpoint Protection Manager files.  
 The default pathname is C:\Program Files\Symantec\Symantec Endpoint Protection Manager\data
- 9 Click **Next**.
- 10 Click **Microsoft SQL Server**.
- 11 Click **Next**.
- 12 Type the name of the database server in the Database server box, if applicable.  
 Type the IP address or host name of the database server where the SQL Server Enterprise Manager (SEM) server saves application data.
- 13 Type the number of the SQL server port in the SQL server port box.  
 The default port number is 1433.
- 14 Type the name of the database in the Database Name box.  
 The name of the Microsoft SQL database where application data is stored.
- 15 Type the name of the user in the User box  
 This name represents the user who is responsible for the database.
- 16 Type the password in the Password field.  
 This password is for the database user. This field cannot be blank.
- 17 Type the name of the SQL client path in the SQL Client Path.  
 By default, the SQL client bin folder contains the bcp.exe file. For example, C:\Program Files\Microsoft SQL Server\80\Tools\Binn.  
 The bcp.exe file must reside on the same computer as the one on which you installed the Symantec Endpoint Protection Manager. This file is part of the SQL Server client package. You must also correctly specify the MS SQL Client pathname in the Management Server Configuration Wizard. If the pathname is not specified correctly or the MS SQL Client package was never installed, then you cannot reconfigure the database.

**18** Click **Next**.

The database is then created. This process only takes a few minutes. A database message appears during that period of time if the Symantec Endpoint Protection Manager service is still running.

**19** You can select to Start Symantec Endpoint Protection Manager and Start Management Console.

These options are selected by default.

**20** Click **Finish**.

You completed the reconfiguration of the database. If you kept the start options selected, the Symantec Endpoint Protection Manager console logon appears.

## Reconfiguring an embedded database

You need to use the Symantec Management Server Configuration Wizard to reconfigure the database.

See [“About the reconfiguration of a database”](#) on page 262.

### To reconfigure an embedded database

- 1** Stop the Symantec Endpoint Protection Manager service by selecting **Start > Programs > Administrative Tools > Services**.
- 2** Locate the Symantec Endpoint Protection Manager and then right-click to select **Stop**.
- 3** Click **Start > Programs > Symantec Endpoint Protection Manager > Management Server Configuration Wizard**.
- 4** In the Welcome to the Management Server Configuration Wizard screen, click **Reconfigure the management server**.
- 5** Click **Next** to begin the reconfiguration.
- 6** Edit the name of the computer on which the Symantec Endpoint Protection Manager is installed in the Server name box.
- 7** Edit the HTTPS port number that the Symantec Endpoint Protection Manager listens on in the Server port box.

The default port number is 8443.

- 8 Edit the location of the server data folder or browse to the root folder where data files are located.

The root folder includes backups, replication, and other Symantec Endpoint Protection Manager files.

The default pathname is C:\Program Files\Symantec\Symantec Endpoint Protection Manager\data

- 9 Click **Next**.

- 10 Click **Embedded database**.

- 11 Click **Next**.

- 12 Type the number of the server port in the Database server port box.

The default port number is 2638.

- 13 Type the password in the Password box.

This field cannot be blank.

- 14 Type the password again the Confirm Password box.

- 15 Click **Next**.

The database creation takes a few minutes. A database message appears during that period of time if the Symantec Endpoint Protection Manager service is still running.

- 16 You can choose to Start Symantec Endpoint Protection Manager and Start Management Console.

These options are selected by default.

- 17 Click **Finish**.

You completed the reconfiguration of the database. If you kept the start options selected, the Symantec Endpoint Protection Manager console logon appears.

## About managing log data

You can configure a number of options to manage the logs that are stored in the database.

### About log data and storage

The data from all the logs that are uploaded to the console are stored in the console database.

Data is stored in two tables in the database from the following types of logs:

- Application and Device Control logs
- Audit log
- Enforcer logs
- Network Threat Protection logs
- System logs

The data from the other logs is stored in a single table.

You can set the log options for managing the database logs that are stored in two tables.

See [“Configuring log settings for the servers in a site”](#) on page 277.

The single table that contains the other logs' data is managed by using the database maintenance options in the site properties. You can set the database maintenance options that affect the data that is stored in a single table.

See [“Configuring database maintenance options for logs”](#) on page 283.

For the logs that are stored in two tables, one table (table A) is the current log table. New log entries are written into this table. When the log threshold or expiration occurs, new log entries are stored in the second table (table B). The data remains in table A until table B reaches its threshold or the number of days that is specified in the Expired after field. At that time, table A is cleared completely and new entries are stored there. The information in table B remains until the switch occurs. Switching from one table to the other, also called sweeping the logs from the database, occurs automatically. The timing of the switch depends on the log settings that you set in the site properties. The process is the same regardless of whether the sweep is automatic or manual.

You can perform a manual log sweep after backing up the database, if you prefer to use this method as part of routine database maintenance.

If you allow an automatic sweep to occur, you may lose some log data if your database backups do not occur frequently enough. If you regularly perform a manual log sweep after you have performed a database backup, it ensures that you retain all your log data. This procedure is very useful if you must retain your logs for a relatively long period of time, such as a year.

---

**Note:** The manual procedure that is described in [Sweeping log data from the database manually](#) does not affect the data in the logs that are stored in a single table in the database.

---

## Sweeping log data from the database manually

You can manually clear the logs, but this procedure is optional and you do not have to do it.

### To sweep log data from the database manually

- 1 To prevent an automatic sweep of the database until after a backup occurs, increase the Site Properties Log Settings to their maximums.

See “[Configuring log settings for the servers in a site](#)” on page 277.

- 2 Perform the backup, as appropriate.
- 3 On the computer where the manager is installed, open a Web browser and type the following URL:

**`https://localhost:8443/servlet/ConsoleServlet?ActionType=ConfigServer&action=SweepLogs`**

After you have performed this task, the log entries for all types of logs are saved in the alternate database table. The original table is kept until the next sweep is initiated.

- 4 To empty all but the most current entries, perform a second sweep. The original table is cleared and entries then start to be stored there again.
- 5 Remember to return the Site Properties Log Settings to your preferred values.

## Log data from legacy clients

The Symantec Endpoint Protection reporting functions use a temporary folder, *drive:\Symantec\Symantec Endpoint Protection Manager\Inetpub\Reporting\Temp*, for several purposes. Some administrators may want to schedule their own automated tasks to periodically clean this temporary folder. If you do so, be sure that you do not delete the *LegacyOptions.inc* file, if it exists. If you delete this file, you lose the incoming data from legacy Symantec AntiVirus client logs.

## Configuring log settings for the servers in a site

To help control disk space usage, you can configure the number of entries that are kept on the server in a site's logs. You can also configure the number of days the entries are kept. You can configure different settings for the different sites.

---

**Note:** Log information on the console Logs tab on the Monitors page is presented in logical groups for you to view. The log names on the Site Properties Log Settings tab correspond to log content rather than to log types on the Monitors page Logs tab.

---

For a description of each configurable option, you can click **Tell me more** for that type of report on the console. **Tell me more** displays the context-sensitive help.

**To configure log settings for the servers in a site**

- 1 In the console, click **Admin**.
- 2 On the lower left, click **Servers**.
- 3 Select the site you want to configure.
- 4 Under Tasks, click **Edit Site Properties**.
- 5 On the Log Settings tab, set the number of entries and number of days to keep log entries for each type of log.

You can set sizes for management server logs, client logs, and Enforcer logs.

- 6 Click **OK**.

## About configuring event aggregation

You configure event aggregation for client logs in two locations on the console.

[Table 20-1](#) describes where to configure client event aggregation and what the settings mean.

**Table 20-1** Client event aggregation

Location	Description
On the Policies page, Antivirus and Antispyware policy, Miscellaneous, Log Handling tab	Use this location to configure the aggregation for risk events. The default aggregation time is 5 minutes. The first occurrence of an event is immediately logged. Subsequent occurrences of the same events are aggregated and the number of occurrences is logged on the client every 5 minutes.
On the Clients page, Policies page, Client Log Settings	Use this location to configure the aggregation of Network Threat Protection events. Events are held on the clients for the damper period before they are aggregated into a single event and then uploaded to the console. The damper period helps to reduce events to a manageable number. The default damper period setting is Auto (Automatic). The damper idle period determines the amount of time that must pass between log entries before the next occurrence is considered a new entry. The default damper idle is 10 seconds.

See [“Setting up log handling parameters in an Antivirus and Antispyware Policy”](#) on page 375.

See “[Configuring client log settings](#)” on page 279.

## Configuring client log settings

If you have installed Symantec Endpoint Protection, you can configure some client log options. You can configure the number of entries kept in the logs and the number of days that each entry is kept on the client.

You can configure settings for the following client logs:

- Control
- Packet
- Risk
- Security
- System
- Traffic

If you have Symantec Network Access Control installed, you can enable and disable logging, and send Enforcer logs to the management server. You can also configure the number of log entries and the number of days the entries are kept on the client.

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

For the Security, Risk, and Traffic logs, you can also configure the damper period and the damper idle period to be used for event aggregation.

You can configure whether or not to upload each type of client log to the server, and the maximum size of the uploads.

If you choose not to upload the client logs, it has the following consequences:

- You cannot view the client log data from the console by using the Logs tab on the Monitoring pane.
- You cannot back up the client logs when you back up the database.
- You cannot export the client log data to a file or a centralized log server.

### To configure client log settings

- 1 On the console, click **Clients**.
- 2 On the Policies tab, under Location-independent Policies and Settings, under Settings, click **Client Log Settings**.
- 3 In the Client Log Settings for *group name* dialog box, set the maximum file size and the number of days to keep log entries.

- 4 Check **Upload to management server** for any logs that you want the clients to forward to the server.
- 5 For the Security log and Traffic log, set the damper period and the damper idle period.  
  
These settings determine how frequently Network Threat Protection events are aggregated.
- 6 Set the maximum number of entries that you want a client to upload to the manager at a time.
- 7 Click **OK**.

## About configuring client log handling options for antivirus and antispysware policies

You can configure the following log handling options for antivirus and antispysware policies:

- Which antivirus and antispysware events are forwarded from clients to the Antivirus and Antispysware Protection logs on the server
- How long the events in the Antivirus and Antispysware Protection logs are retained on the server
- How frequently aggregated events are uploaded from clients to the server

See [“Setting up log handling parameters in an Antivirus and Antispysware Policy”](#) on page 375.

## Backing up the logs for a site

Log data is not backed up unless you configure Symantec Endpoint Protection to back it up. If you do not back up the logs, then only your log configuration options are saved during a backup. You can use the backup to restore your database, but the logs in the database are empty of data when they are restored.

This configuration option is located with the other backup options for local sites on the Servers page of the Admin page. You can choose to keep up to ten versions of site backups. You should ensure that you have adequate disk space to keep all your data if you choose to keep multiple versions.

### To back up the logs for a site

- 1 On the console, click **Admin**.
- 2 Select a database server.
- 3 Under Tasks, click **Edit Backup Settings**.



- 4 In the Backup Settings group box, check **Back up logs**.
- 5 Click **OK**.

## About uploading large amounts of client log data

If you have a large number of clients, you may have a large volume of client log data.

You should consider whether or not you want to reduce the volume of data by using the following configurations:

- Upload only some of the client logs to the server.  
See [“Configuring client log settings”](#) on page 279.
- Filter the less important risk events and system events out so that less data is forwarded to the server.  
See [“Setting up log handling parameters in an Antivirus and Antispyware Policy”](#) on page 375.

If you still plan to upload very large amounts of client log data to a server, you need to consider the following factors:

- The number of clients in your network
- The heartbeat frequency, which controls how often the client logs are uploaded to the server
- The amount of space in the directory where the log data is stored before being inserted into the database

A configuration that uploads a large volume of client log data to the server at frequent intervals can cause space problems. If you must upload a large volume of client log data, you may have to adjust some default values to avoid these space problems. As you deploy to clients, you should monitor the space on the server in the log insertion directory and adjust these values as needed. The default directory where the logs are converted to .dat files and then written into the database is `drive:\Program Files\Symantec\Symantec Endpoint Protection Manager\data\inbox\log`. The location of the server data directory is set during installation when you are asked to select the server data folder. You can run the Management Server Configuration Wizard from the Start menu to change this directory if desired. The `\inbox\log` directory is automatically added to the directory you set.

The frequency with which the client logs are uploaded is configured on the Policies page of the Clients page, under Communications Settings. The default frequency is to upload the logs every five minutes.

To adjust the values that control the space available on the server, you must change these values in the registry. The registry keys that you need to change are located on the server in HKEY\_LOCAL\_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\SEPM.

Table 20-2 lists the registry keys and their default values and describes what they do.

**Table 20-2** Registry keys that contain log upload settings

Value name	Default and description
MaxInboxSpace	MaxInboxSpace specifies the space that is allotted for the directory where log files are converted to .dat files before they are stored in the database.  The default value is 200 MB.
MinDataFreeSpace	MinDataFreeSpace specifies the minimum amount of space that should be kept free in this directory. This key is useful to ensure that other applications that use the same directory have enough space to run without an adverse effect on performance.  The default value is 0.
IntervalOfInboxSpaceChecking	IntervalOfInboxSpaceChecking specifies how long Symantec Endpoint Protection waits between checks on the amount of space in the inbox that is available for log data.  The default value is 30 seconds.

## About managing log events in the database

The database receives and stores a constant flow of entries into its log files. You must manage the data that are stored in the database so that the stored data does not consume all the available disk space. Too much data can cause the computer on which the database runs to crash.

You should understand your default database maintenance settings and change them if the disk space that the database uses seems to grow constantly. If there is a large spike in risk activity, you may need to delete some data to protect the available disk space on the server.

## Configuring database maintenance options for logs

Administrators can configure database maintenance options for the data that are stored in the logs. Database maintenance options help you to manage the size of your database by specifying compression settings and how long to keep data.

For information about the specific database maintenance options, refer to the context-sensitive help on the Site Properties for *site name* dialog box Database tab.

### To configure database maintenance options for logs

- 1 On the console, click **Admin**.
- 2 Select a site.
- 3 Under Tasks, click **Edit Site Properties**.
- 4 On the Database tab, set the number of days to keep risk events.  
To retain the subset of risk infection events after the threshold that you set for risk events, check the **Do not delete infection events** check box.
- 5 Set how frequently you want to compress identical risk found events into a single event.
- 6 Set the number of days to keep the events that have been compressed.  
This value includes the time before the events were compressed. For example, suppose that you specify to delete compressed events after ten days and specify to compress events after seven days. In this case, the events are deleted three days after they are compressed.
- 7 Set the number of days to keep acknowledged and unacknowledged notifications.
- 8 Set the number of days to keep scan events.
- 9 Set the number of days to keep commands that you have run from the console and their associated command status information. After this time, Symantec Endpoint Protection can no longer distribute the commands to their intended recipients.
- 10 Check the check boxes if you want to delete unused virus definitions and the virus events that contain EICAR as the name of the virus.  
The EICAR test virus is a text file that the European Institute for Computer Anti-Virus Research (EICAR) developed. It provides an easy and safe way to test most antivirus software. You can download it from the EICAR Web site. You can use it to verify that the antivirus portion of Symantec Endpoint Protection works.
- 11 Click **OK**.

## About using the Interactive SQL utility with the embedded database

If you choose to use the embedded database with Symantec Endpoint Protection or Symantec Network Access Control, you should note the following information. When you run the database application named Interactive SQL (dbisqlc.exe), it blocks the insertion of data into the embedded database. If you use the application for a while, .dat files accumulate in the *drive*:\Program Files\Symantec\Symantec Endpoint Protection Manager\data\inbox\log directories. To alleviate the buildup of the .dat files and restart data insertion into the database, close the application.

## Changing timeout parameters

If database errors occur when you view reports or logs that contain a lot of data, you can make the following changes:

- Change the Microsoft SQL server connection timeout
- Change the Microsoft SQL server command timeout

The reporting defaults for these values are as follows:

- Connection timeout is 300 seconds (5 minutes)
- Command timeout is 300 seconds (5 minutes)

If you get CGI or terminated process errors, you might want to change other timeout parameters. See the Symantec Knowledge Base article called "Reporting server does not report or shows a timeout error message when querying large amounts of data."

### To change timeout parameters

- 1 Open the Reporter.php file, which is located in the \Program Files\Symantec\Symantec Endpoint Protection Manager\Inetpub\Reporting\Resources directory.
- 2 Use any text editor to add the following settings to the file:
  - **\$CommandTimeout =xxxx**
  - **\$ConnectionTimeout =xxxx**Timeout values are in seconds. If you specify zero, or leave the fields blank, the default settings are used.

## About recovering a corrupted client System Log on 64-bit computers

If the System Log becomes corrupted on a 64-bit client, you may see an unspecified error message in the system logs on the console. If corrupted, you cannot view the data in the log on the client and the data does not upload to the console. This

condition can affect data in the console Computer Status, Risk, and Scan logs and reports.

To correct this condition, you can delete the corrupted log file and the `serialize.dat` file on the client. These files are located on the client in `Drive:\Documents and Settings\All Users\Application Data\Symantec\Symantec AntiVirus Corporate Edition\7.5\Logs\date.Log`. After you delete these files, the log file is recreated and begins to log entries correctly.



# Replicating data

This chapter includes the following topics:

- [About the replication of data](#)
- [Understanding the impact of replication](#)
- [Setting up data replication](#)
- [Scheduling automatic and on-demand replication](#)
- [Replicating client packages](#)
- [Replicating logs](#)

## About the replication of data

Replication is the process of sharing information between databases to ensure that the content is consistent. You can use replication to increase the number of database servers that are available to clients and thereby reduce the load on each. Replication is typically set up during the initial installation.

See the *Installation Guide for Symantec Endpoint Protection and Symantec Network Access Control* for more information on how to set up data replication during an initial installation.

A replication partner is another site with one database server. It also has a connection to the site that you designate as a main site or a local site. A site may have as many replication partners as needed. All replication partners share a common license key. The changes that you made on any replication partner are duplicated to all other replication partners whenever Symantec Endpoint Protection Manager is scheduled to replicate data.

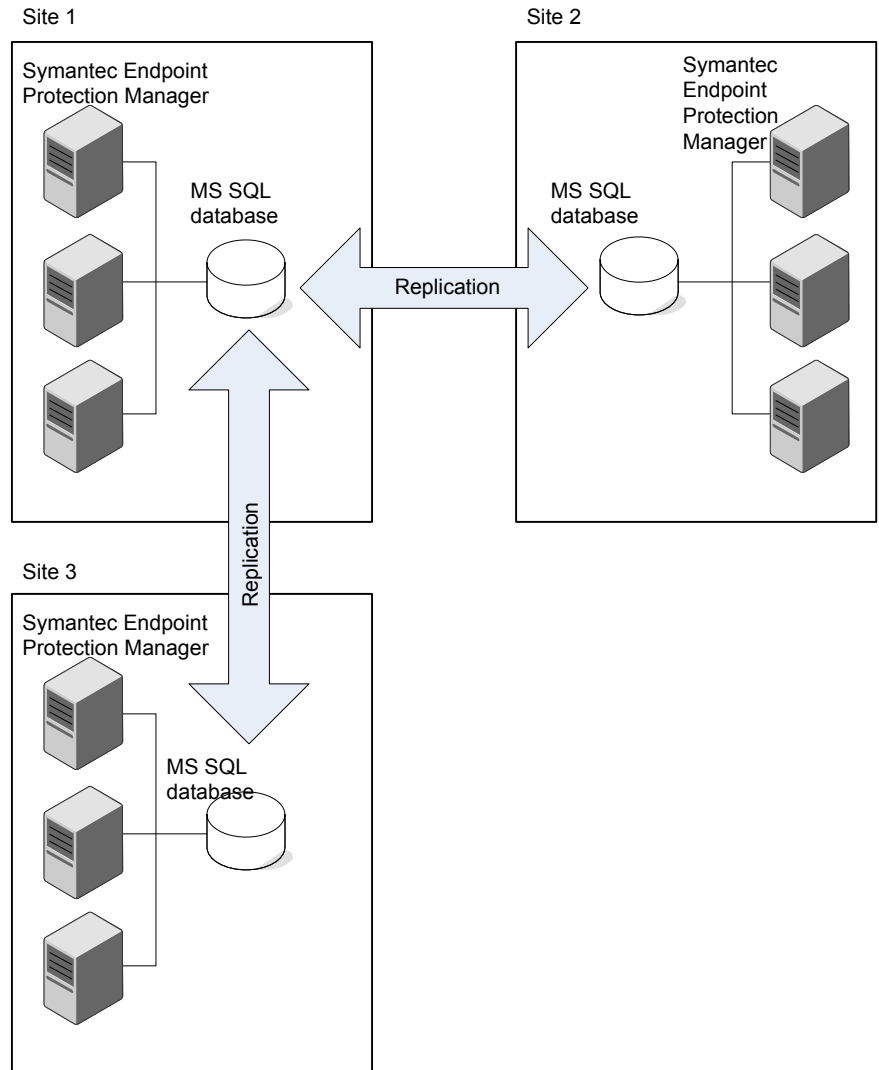
For example, you may want to set up one site at your main office (site 1) and a second site (site 2). Site 2 is a replication partner to the first site. The databases

on site 1 and site 2 are reconciled by using a synchronization schedule that you must set up. If a change is made on site 1, it automatically appears on site 2 after replication occurs. If a change is made on site 2, it automatically appears on site 1 after replication occurs. You can also install a third site (site 3) that can replicate data from either site 1 or site 2. The third site is a replication partner to the other two sites.

[Figure 21-1](#) illustrates how replication of data occurs from a local site to two other sites.



Figure 21-1 Site Replication Partners



Replication partners are listed on the Admin page. You can display information about replication partners by selecting the partner in the tree. All sites typically have the same type of database. You can, however, set up replication between sites by using different types of databases. In addition, you can also set up replication between an embedded database and an MS SQL database.

If you use an embedded database, you can only connect one Symantec Endpoint Protection Manager to it because of configuration requirements. If you use an MS SQL database, you can connect multiple Symantec Endpoint Protection Managers or share one database. Only the first Symantec Endpoint Protection Manager needs to be set up as a replication partner.

All sites that are set up as replication partners are considered to be on the same site farm. Initially, you install the first site, then install a second site as a replication partner. A third site can be installed and set up to connect to either of the first two sites. You can add as many sites as needed to the site farm.

You can delete replication partners to stop the replication. Later you can add that replication partner back to make the databases consistent. However, some changes may collide.

See [“What settings are replicated”](#) on page 290.

## Understanding the impact of replication

If administrators make changes on at each replication site simultaneously, some changes may get lost. If you change the same setting on both sites and a conflict arises, the last change is the one that takes effect when replication occurs.

For example, site 1 (New York) replicates with site 2 (Tokyo) and site 2 replicates with site 3 (London). You want the clients that connect to the network in New York to also connect with the Symantec Endpoint Protection Manager in New York. However, you do not want them to connect to the Symantec Endpoint Protection Manager in either Tokyo or London.

## What settings are replicated

When you set up replication, client communication settings are also replicated. Therefore, you need to make sure that the communication settings are correct for all sites on the site farm in the following manner:

- Create generic communication settings so that a client's connection is based on the type of connection. For example, you can use a generic DNS name, such as `symantec.com` for all sites on a site farm. Whenever clients connect, the DNS server resolves the name and connects the client to the local Symantec Endpoint Protection Manager.
- Create specific communication settings by assigning groups to sites so that all clients in a group connect to a designated Symantec Endpoint Protection Manager.

For example, you can create two groups for clients at site 1, two different groups for site 2, and two other groups for site 3. You can apply the

communication settings at the group level so clients connect to the designated Symantec Endpoint Protection Manager.

You may want to set up guidelines for managing location settings for groups. Guidelines may help prevent conflicts from occurring on the same locations. You may also help prevent conflicts from occurring for any groups that are located at different sites.

## How changes are merged during replication

After replication occurs, the database on site 1 and the database on site 2 are the same. Only computer identification information for the servers differs.

If administrators change settings on all sites on a site farm, conflicts can occur. For example, administrators on site 1 and site 2 can both add a group with the same name. If you want to resolve this conflict, both groups then exist after replication. However, one of them is renamed with a tilde and the numeral 1 (~1).

If both sites added a group that is called Sales, after replication you can see two groups at both sites. One group is called Sales and the other is called Sales 1. This duplication occurs whenever a policy with the same name is added to the same place at two sites.

If duplicate network adapters are created at different sites with the same name, a tilde and the numeral 1 (~1) is added. The two symbols are added to one of the names.

If different settings are changed at both sites, the changes are merged after replication. For example, if you change Client Security Settings on site 1 and Password Protection on site 2, both sets of changes appear after replication. Whenever possible, changes are merged between the two sites.

If policies are added at both sites, new policies appear on both sites after replication. Conflicts can occur when one policy is changed at two different sites. If a policy is changed at multiple sites, the last update of any change is then maintained after replication.

If you perform the following tasks with the replication that is scheduled to occur every hour on the hour:

- You edit the AvAsPolicy1 on site 1 at 2:00 P.M.
- You edit the same policy on site 2 at 2:30 P.M.

Then only the changes that have been completed on site 2 appear after replication is complete when replication occurs at 3:00 P.M.

If one of the replication partners is taken offline, the remote site may still indicate the status as online.

## Setting up data replication

You can set up data replication during the initial installation or at a later time. When you set up replication during the initial installation, you can also set up a schedule for the synchronization of the replication partners.

### Adding replication partners and schedule

If you want to replicate data with another site, you may have already set it up during the initial installation. If you did not set up replication during the initial installation, you can do so now by adding a replication partner. Multiple sites are called a site farm whenever they are set up as replication partners. You can add any site on the site farm as a replication partner.

See the *Installation Guide for Symantec Endpoint Protection and Symantec Network Access Control* for more information.

Also, you can add a replication partner that was previously deleted as a partner.

Before you begin, you need to have the following information:

- An IP address or host name of the Symantec Endpoint Protection Manager for which you want to make a replication partner.
- The Symantec Endpoint Protection Manager to which you want to connect must have previously been a replication partner. The Symantec Endpoint Protection Manager can have also been a partner to another site on the same site farm.

#### To add a replication partner

- 1 In the Symantec Endpoint Protection Manager console, click **Admin**.
- 2 Under View Servers, select a site.
- 3 In the Admin page, under Tasks, click **Add Replication Partner**.
- 4 In the Add Replication Partner wizard, click **Next**.
- 5 Type the IP address or host name of the Symantec Endpoint Protection Manager that you want to make a replication partner.
- 6 Type the port number of the remote server on which you installed the Symantec Endpoint Protection Manager.  
The default setting for the remote server port is 8443.
- 7 Type the administrator's user name and password.
- 8 Click **Next**.

- 9 In the Schedule Replication pane, specify the schedule for replication between the two partners by doing one of the following:
  - Check **Autoreplicate**.  
It causes frequent and automatic replication to occur between two sites. This option is the default setting. Therefore you cannot set up a custom schedule for replication.
  - Uncheck **Autoreplicate**  
You can now set up a custom schedule for replication:
    - Select the hourly, daily, or weekly **Replication Frequency**.
    - Select the specific day during which you want replication to occur in the **Day of Week** list to set up a weekly schedule.
- 10 Click **Next**.
- 11 In the Replication of Log Files and Client Packages pane, check or uncheck the options depending on whether or not you want to replicate logs.  
The default setting is unchecked.
- 12 Click **Next**.
- 13 Click **Finish**.  
The replication partner site is added under Replication Partners on the Admin page.

## Disconnecting replication partners

Deleting a replication partner merely disconnects a replication partner from the Symantec Endpoint Protection Manager. It does not delete the site. You can add the site back later if you need to do so by adding a replication partner.

### To remove databases from the replication process

- 1 In the Symantec Endpoint Protection Manager console, click **Admin**.
- 2 In the Admin page, under View, click **Replication Partners**.
- 3 Expand **Replication Partners** and select the partner from which you want to disconnect.
- 4 In the Admin page, under asks pane, click **Delete Replication Partner**.
- 5 Type **Yes** when asked to verify that you want to delete the replication partner.

# Scheduling automatic and on-demand replication

You can schedule replication automatically or on demand. You can also specify the frequency with which you want to schedule replication.

## Replicating data on demand

Replication normally occurs according to the schedule that you set up when you added a replication partner during installation. The site with the smaller ID number initiates the scheduled replication. At times, you may want replication to occur immediately.

### Scheduling on-demand replication

- 1 In the Symantec Endpoint Protection Manager console, click **Admin**.
- 2 In the Admin page, click **Servers**.
- 3 In the Admin page, under View, expand **Replication Partners** and select the partner whose database you want to replicate immediately.
- 4 In the Admin page, under Tasks, click **Replicate Now**.
- 5 Click **Yes** when asked to verify that you want to start a one time replication now.

The following message appears:

```
Replication has been scheduled.  
For details regarding the outcome of the scheduled  
event, please check the server system logs after  
a few minutes delay. The delay depends on the load  
of the server, the amount of changes to be replicated,  
and the bandwidth of the communication channel.
```

- 6 Click **OK**. The database is replicated immediately.

If you use a Microsoft SQL database with more than one server, you can only initiate replication from the first server at that site. If you try to replicate now from the second server, the following message appears:

```
Only the first server of the site can perform the replication.  
Please log on to the server: <first server name> to start  
replication.
```

## Changing replication frequencies

Replication normally occurs according to the schedule that you set up when you added a replication partner during the initial installation. The site with the smaller ID number initiates the scheduled replication. When a replication partner has been established, you can change the replication schedule. When you change the schedule on a replication partner, the schedule on both sides is the same after the next replication.

### To change replication frequencies

- 1 In the Symantec Endpoint Protection Manager console, click **Admin**.
- 2 In the Admin page, under View, click **Replication Partners**.
- 3 In the Admin page, under Tasks, click **Edit Replication Partner**.
- 4 In the Edit Replication Partner dialog box, specify the schedule for replication between the two partners by doing one of the following:
  - Check **Autoreplicate**.  
It causes frequent and automatic replication to occur between two sites. This option is the default setting. Therefore you cannot set up a custom schedule for replication.
  - Uncheck **Autoreplicate**  
You can now set up a custom schedule for replication.
    - Select the hourly, daily, or weekly **Replication Frequency**.
    - Select the specific day during which you want replication to occur in the **Day of Week** list to set up a weekly schedule.
- 5 Click **OK**.

## Replicating client packages

You can choose to replicate or duplicate client packages between the local site and a replication partner at a remote site. You may want to copy the latest version of a client package from a local site to a remote site. The administrator at the remote site can then deploy the client package.

See the *Installation Guide for Symantec Endpoint Protection and Symantec Network Access Control* for more information on how to create and deploy client installation packages at a site.

If you decide to replicate client packages, you may duplicate a large volume of data. Should you replicate many packages, the data may be as large as 5 GB. Both

Symantec Endpoint Protection and Symantec Network Access Control 32-bit and 64-bit installation packages may require as much as 500 MB of disk space.

See the *Installation Guide for Symantec Endpoint Protection and Symantec Network Access Control* for more information about requirements for disk storage.

#### To replicate client packages between replication partners

- 1 In the Symantec Endpoint Protection Manager console, click **Admin**.
- 2 In the Admin page, under View, click **Replications Partners**.
- 3 Expand **Replication Partners** and select the replication partner with which you want to replicate client packages.
- 4 In the Admin page, under Tasks, click **Edit Replication Partner Properties**.
- 5 In the Replication Partner Properties dialog box, under Partner, click **Replicate client packages between local site and partner site**.
- 6 Click **OK**.

## Replicating logs

You can specify that you want to replicate or duplicate logs as well as the database of a replication partner. You can specify the replication of logs when adding replication partners or by editing the replication partner properties. If you plan to replicate logs, make sure that you have sufficient disk space for the additional logs on all the replication partner computers.

See [“Viewing logs from other sites”](#) on page 181.

#### To replicate logs between replication partners

- 1 In the Symantec Endpoint Protection Manager console, click **Admin**.
- 2 In the Admin page, under View, click **Replications Partners**.
- 3 Expand **Replication Partners** and select the replication partner for which you want to start generating replication logs.
- 4 In the Admin page, under Tasks, click **Edit Replication Partner Properties**.
- 5 In the Replication Partner Properties dialog box, under Partner, click **Replicate logs from local site to this partner site** or **Replicate logs from this partner site to local site**.
- 6 Click **OK**.



# Managing Tamper Protection

This chapter includes the following topics:

- [About Tamper Protection](#)
- [Configuring Tamper Protection](#)

## About Tamper Protection

Tamper Protection provides real-time protection for Symantec applications that run on servers and clients. It prevents non-Symantec processes such as worms, Trojan horses, viruses, and security risks, from affecting Symantec processes. You can configure the software to block or log attempts to modify Symantec processes.

---

**Note:** If you use third-party security risk scanners that detect and defend against unwanted adware and spyware, these scanners typically impact Symantec processes. If you have Tamper Protection enabled when you run such a scanner, Tamper Protection generates a large number of notifications and log entries. A best practice for Tamper Protection is to always leave it enabled. Use log filtering if the number of the events generated is too large.

---

When a client is installed as an unmanaged client, Tamper Protection has the following default values:

- Tamper Protection is enabled.
- The action that Tamper Protection takes when it detects a tamper attempt is to block the attempt and log the event.

- Tamper Protection sends the user a default message when it detects a tamper attempt.

When a client is installed as a managed client, Tamper Protection has the following default values:

- Tamper Protection is enabled.
- The action that Tamper Protection takes when it detects a tamper attempt is to log the event only.
- Tamper Protection does not send the user a message when it detects a tamper attempt.

---

**Note:** If you enable notifications when Symantec Endpoint Protection detects a tamper attempts, notifications about Windows processes are sent to affected computers as well as notifications about Symantec processes.

---

## Configuring Tamper Protection

You can enable and disable Tamper Protection and configure the action that it takes when it detects a tampering attempt. You can also configure it to notify users when it detects a tampering attempt.

A best practice when you initially use Symantec Endpoint Protection is to use the action Log the event only while you monitor the logs once a week. When you are comfortable that you see no false positives, then set Tamper Protection to Block it and log the event.

You can configure a message to appear on clients when Symantec Endpoint Protection detects a tamper attempt. By default, notification messages appear when the software detects a tamper attempt.

The message that you create can contain a mix of text and variables. The variables are populated with the values that identify characteristics of the attack. If you use a variable, you must type it exactly as it appears.

[Table 22-1](#) describes the variables you can use to configure a message.

**Table 22-1** Tamper Protection message variables and descriptions

Field	Description
[ActionTaken]	The action that Tamper Protection performed to respond to the attack.
[ActorProcessID]	The ID number of the process that attacked a Symantec application.

**Table 22-1** Tamper Protection message variables and descriptions (*continued*)

Field	Description
[ActorProcessName]	The name of the process that attacked a Symantec application.
[Computer]	The name of the computer that was attacked.
[DateFound]	The date on which the attack occurred.
[EntityType]	The type of target that the process attacked.
[Filename]	The name of the file that attacked the protected processes.
[Location]	The area of the computer hardware or software that was protected from tampering. For Tamper Protection messages, this field is Symantec applications.
[PathAndFilename]	The complete path and name of the file that attacked protected processes.
[SystemEvent]	The type of the tamper attempt that occurred.
[TargetPathname]	The location of the target that the process attacked.
[TargetProcessID]	The process ID of the target that the process attacked.
[TargetTerminalSession ID]	The ID of the terminal session during which the event occurred.
[User]	The name of the logged on user when the attack occurred.

#### To enable or disable Tamper Protection

- 1 In the console, click **Clients**.
- 2 On the Policies tab, under Settings, click **General Settings**.
- 3 On the Tamper Protection tab, check or uncheck **Protect Symantec security software from being tampered with or shut down**.
- 4 Click the lock icon if you do not want users to be able to change this setting.
- 5 Click **OK**.

#### To configure basic Tamper Protection settings

- 1 In the console, click **Clients**.
- 2 On the Policies tab, under Settings, click **General Settings**.
- 3 On the Tamper Protection tab, in the list box, select one of the following actions:

- To block and log unauthorized activity, click **Block it and log the event**.
  - To log unauthorized activity but allow the activity to take place, click **Log the event only**.
- 4 Click the lock icon if you do not want users to be able to change this setting.
  - 5 Click **OK**.

**To enable and customize Tamper Protection notification messages**

- 1 In the console, click **Clients**.
- 2 On the Policies tab, under Settings, click **General Settings**.
- 3 On the Tamper Protection tab, click **Display a notification message when tampering is detected**.
- 4 In the text field box, if you want to modify the default message, you can type additional text and delete text.  
  
If you use a variable, you must type it exactly as it appears.
- 5 Click the lock icon if you do not want users to be able to change this setting.
- 6 Click **OK**.

# General policy management tasks

- [About policies](#)
- [Managing a group's inheritance for locations and policies](#)
- [Managing a group's locations](#)
- [Working with policies](#)
- [Pushing and pulling policies between management servers, clients, and optional Enforcers](#)
- [Setting up learned applications](#)



# About policies

This chapter includes the following topics:

- [Overview of policies](#)
- [About shared and non-shared policies](#)
- [About policy-related tasks](#)
- [Groups, inheritance, locations, and policies](#)
- [Examples of policies](#)

## Overview of policies

The Policies page on the Symantec Endpoint Protection Manager console provides a centrally managed solution. It handles security policy enforcement, Host Integrity checking (Symantec Network Access Control only), and automated remediation over all clients. The policies functionality is the heart of the Symantec software. Clients connect to the server to get the latest policies, security settings, and software updates.

You can also perform many of the policy-related tasks on the Clients page. You typically perform most policy-related tasks for shared policies in the Policies page. However, you perform most of the policy-related tasks for non-shared tasks in the Clients page.

Symantec Endpoint Protection Manager learns communications behavior, creates and deploys security and enforcement policies, manages user and computer group structures, and communicates with other management servers. Through Symantec's heartbeat communication protocol, the management server learns about user, application, and network behavior from clients. The management server provides enterprises with an up-to-the-minute view of their security status.

You can use several types of policies to manage the corporate environment. Some of these policies are automatically created during the installation. You can use a default policy as is or further customize it to suit a specific corporate environment.

[Table 23-1](#) lists each policy, whether or not a default policy is created during the initial installation, and a description for each policy.

**Table 23-1** Symantec Endpoint Protection Manager policies

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

Enterprises use the information that the management server collects to create security policies. These security policies link users, connectivity technology,



applications, and network communication to security policies. Symantec's security policies are managed and inherited through group structures of users, computers, and servers. You can import information about users and computers. You can also synchronize data with directory servers, such as Active Directory and LDAP. The management server can be centralized or distributed in a global enterprise to provide scalability, fault tolerance, load balancing, and policy replication.

You can perform the following tasks:

- Set up your administrative structure and organizational structure, which includes computers, users, and groups.
- Set up security policies.  
Each group that you define as part of your organizational structure can have a separate policy. You can also set up individual policies for locations, such as home and office within a group.
- Set up and deploy client packages.
- Customize client settings.
- Manage Symantec Endpoint Protection Manager sites and replication.
- Configure Symantec Enforcers if you use them as part of your enforcement solution.
- Monitor logs and view reports.

## About shared and non-shared policies

You can create the following types of policies:

Shared policy	Applies to any group and location. You can have multiple shared policies.
Non-shared policy	Applies to a specific location in a group. However, you can only have one policy per location.

You should create shared policies because you can easily edit and replace a policy in all groups and locations that use it. However, you may need a specialized policy for a particular location that already exists. In that case, you can create a policy that is unique to a location.

When you create a new policy, you typically edit a default policy. A default policy always includes default rules and security settings.

You apply a separate policy to each group of users or computers. However, you can also apply separate security policies to each group's location. For example, a group has been assigned multiple locations. Each user may want to connect to an

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

## About policy-related tasks

After you complete the installation of the Symantec Endpoint Protection Manager console, you can customize any of the default policies.

[Table 23-2](#) lists the routine tasks that you must perform when you maintain shared and non-shared policies.

**Table 23-2** Policy management tasks

Name of task	Type of policy
Add	<ul style="list-style-type: none"> <li>■ Antivirus and Antispyware</li> <li>■ Firewall</li> <li>■ Intrusion Prevention</li> <li>■ Host Integrity</li> <li>■ Application and Device Control</li> <li>■ LiveUpdate</li> <li>■ Centralized Exceptions</li> </ul>
Edit	<ul style="list-style-type: none"> <li>■ Antivirus and Antispyware</li> <li>■ Firewall</li> <li>■ Intrusion Prevention</li> <li>■ Host Integrity</li> <li>■ Application and Device Control</li> <li>■ LiveUpdate</li> <li>■ Centralized Exceptions</li> </ul>
Delete	<ul style="list-style-type: none"> <li>■ Antivirus and Antispyware</li> <li>■ Firewall</li> <li>■ Intrusion Prevention</li> <li>■ Host Integrity</li> <li>■ Application and Device Control</li> <li>■ LiveUpdate</li> <li>■ Centralized Exceptions</li> </ul>

**Table 23-2** Policy management tasks (*continued*)

Name of task	Type of policy
Export	<ul style="list-style-type: none"> <li>■ Antivirus and Antispyware</li> <li>■ Firewall</li> <li>■ Intrusion Prevention</li> <li>■ Host Integrity</li> <li>■ Application and Device Control</li> <li>■ LiveUpdate</li> <li>■ Centralized Exceptions</li> </ul>
Assign	<ul style="list-style-type: none"> <li>■ Antivirus and Antispyware</li> <li>■ Firewall</li> <li>■ Intrusion Prevention</li> <li>■ Host Integrity</li> <li>■ Application and Device Control</li> <li>■ LiveUpdate</li> <li>■ Centralized Exceptions</li> </ul> <p><b>Note:</b> You do not assign a non-shared policy, as it is automatically assigned to the location in which you create it.</p>
Withdraw	<ul style="list-style-type: none"> <li>■ Antivirus and Antispyware</li> <li>■ Firewall</li> <li>■ Intrusion Prevention</li> <li>■ Host Integrity</li> <li>■ Application and Device Control</li> <li>■ Centralized Exceptions</li> </ul>
Replace	<ul style="list-style-type: none"> <li>■ Antivirus and Antispyware</li> <li>■ Firewall</li> <li>■ Intrusion Prevention</li> <li>■ Host Integrity</li> <li>■ Application and Device Control</li> <li>■ LiveUpdate</li> <li>■ Centralized Exceptions</li> </ul>

**Table 23-2** Policy management tasks (*continued*)

Name of task	Type of policy
Copy	<ul style="list-style-type: none"> <li>■ Antivirus and Antispyware</li> <li>■ Firewall</li> <li>■ Intrusion Prevention</li> <li>■ Host Integrity</li> <li>■ Application and Device Control</li> <li>■ LiveUpdate</li> <li>■ Centralized Exceptions</li> </ul>
Import	<ul style="list-style-type: none"> <li>■ Antivirus and Antispyware</li> <li>■ Firewall</li> <li>■ Intrusion Prevention</li> <li>■ Host Integrity</li> <li>■ Application and Device Control</li> <li>■ LiveUpdate</li> <li>■ Centralized Exceptions</li> </ul>

## Groups, inheritance, locations, and policies

You can develop shared policies and then you can apply them to specific groups and locations. You can apply policies at the Global group level, a root, or a head group. Subgroups can inherit policies on the Symantec Endpoint Protection Manager console. You can apply one policy with multiple rules to a group or location.

## Examples of policies

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

You may want to implement a restrictive policy regarding the installation of non-certified applications on most employee workstations to protect the enterprise network from attacks. The 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.

# Managing a group's inheritance for locations and policies

This chapter includes the following topics:

- [About groups inheriting locations and policies from other groups](#)
- [Disabling and enabling a group's inheritance](#)

## About groups inheriting locations and policies from other groups

In the group structure, subgroups initially and automatically inherit information about locations, policies, and settings from the parent group. By default, inheritance is enabled for every group. However, you can disable inheritance at any time for any group.

For example, you may want to create a group that is called Engineering with a subgroup that is called Quality Assurance. The Quality Assurance subgroup automatically includes the same locations, policies, and settings as the Engineering group.

If you want to change the policies and settings in the Quality Assurance subgroup, you must first disable inheritance for the Quality Assurance subgroup. If you do not disable inheritance, a message appears at the top of the dialog box of the item that you want to change. This message states that you cannot modify locations, policies, or settings because they are inherited from the Engineering group.

If you create a subgroup and subsequently disable inheritance for this subgroup, nothing in that subgroup changes initially. It maintains all the locations and

policies of the group from which it initially inherited information about its locations and policies.

However, you can make changes to the subgroup that are independent of the group from which it initially inherited information about its locations and policies. If you make changes and later enable inheritance, any changes for the subgroup are overwritten. They are overwritten by the locations and policies that are currently present in the group from which it now inherits its policies.

You may want to assign policies and settings to every group. Therefore you should add them to the group at the highest level before you disable inheritance for a subgroup. Then all the subgroups share the same information about locations and policies, even if you later enable inheritance again.

See [“Adding inherited rules from a parent group”](#) on page 439.

## Disabling and enabling a group's inheritance

You can disable and enable a group's inheritance at any time. By default, inheritance is enabled whenever you create a new location for a group.

### To disable and enable a group's inheritance

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

You can select any group other than the group that is associated with the Temporary group.

- 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.

# Managing a group's locations

This chapter includes the following topics:

- [About a group's locations](#)
- [Enabling a client's automatic assignment of policies](#)
- [Adding a location with a wizard](#)
- [Adding a location without a wizard](#)
- [Assigning a default location](#)
- [Editing the name and description of a group's location](#)
- [Deleting a group's location](#)

## About a group's locations

Policies and settings often need to differ based on the location from which a user tries to connect to the corporate network. Therefore, you can create different locations or profiles for each group of which a user is a member.

You can have many locations, such as the following examples:

- Default (work in a corporate office)
- Remote office (work at a remote corporate facility)
- VPN (VPN from an outside location)
- Home (work from a home location through an Internet service provider)

You can customize the policy and settings of each location according to the specific conditions that are appropriate for that location.

For example, the policies for the default location may not be as strict as the policies for the VPN or home locations. The policy that is associated with the default location is used when the user is already behind a corporate firewall.

You add locations after you have set up all the groups that you need to manage. Each group can have different locations if your security strategy requires it.

If you add a location, it applies to the group for which you created it and any subgroups that inherit from the parent group. Therefore the locations that you intend to apply to all end users should probably be created at the Global group level. Locations specific to a particular group can be created at the subgroup level.

For example, in most companies all end users require a default location that is added automatically to the Global group. However, not all end users require a VPN connection. The end users who require a VPN connection can be organized in a group that is called Telecommuter. You add the VPN location to the Telecommuter group as well as to the inherited office location. Members of that group can then use the policies that are associated with either the office or the VPN location.

## About locations and location awareness

If you want to protect your network, then you need to set up the conditions to trigger this automatic switching or location awareness. You must automatically apply automatically the best security policy to a client or server. The best security policy is typically contingent upon the location from where a user connects.

You can add a set of conditions to each group's location that automatically selects the correct security policy for a user's environment. These conditions are based on information, such as the network settings of the computer from which the request for network access was initiated. An IP address, a MAC address, or the address of a directory server can also function as condition.

If you change a security policy in the console, either the management server updates the policy on the client or the client downloads the policy. If the current location is not valid after the update, then the client switches to another location that is valid or the client uses the default location.

## About planning locations

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

You should consider the following questions:

- From which locations are users connecting?



Consider which locations need to be created and how to label each one. For example, users may connect at the office, from home, from a customer site, or from another remote site such as a hotel during travel. Additional qualified locations may be required at a large site.

- Should location awareness be set up for each location?
- How do you want to identify the location if using location awareness?  
You can identify the location based on IP addresses, WINS, DHCP, or DNS server addresses, network connections, and other criteria.
- If you identify the location by network connection, what type of connection is it?  
For example, the network connection may be a connection to the Symantec Endpoint Protection Manager, dial-up networking, or a particular brand of VPN server.
- Do you want clients connecting in this location to use a specific type of control, such as server control, mixed control, or client control?
- Do you want to do Host Integrity checks at each location? Or do you want to skip it at any time such as when not connected to the Symantec Endpoint Protection Manager?
- What applications and services should be allowed at each location?
- Do you want the location to use the same communication settings as the other locations in the group or to use different ones? You can set unique communication settings for one location.

## About a group's default location

The default location is used if one of the following cases occurs:

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

When the Symantec Endpoint Protection Manager is initially installed, only the default location, called Default, is set up. At that time, every group's default location is Default. You can change the default location later after you add other locations. Every group must have a default location.

You may prefer to designate a location like Home or Road as the default location.

## Enabling a client's automatic assignment of policies

You can control the policies that are assigned to clients contingent on the location from which a client connects. You should therefore enable location awareness.

### To enable a client's automatic assignment of policies

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

You can modify only the location-independent settings for those groups that have not inherited those policies and setting from a parent group.

- 4 Under Location-independent Policies and Settings, click **General Settings**.
- 5 In the General Settings dialog box, on the General Settings tab, under Location Settings, check **Remember the last location**.

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

- If Remember the last location is checked when a client computer connects to the network, then the client is initially assigned a policy. This policy is associated with 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 in server control. If a quarantine location is enabled, the client may switch to the quarantine policy after a few seconds.
- If Remember the last location is not checked when a client connects to the network, then the client is initially assigned the policy that is associated with 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 in server control. If a quarantine location is enabled, the client may switch to the Quarantine Policy after a few seconds.

**6 Check **Enable Location Awareness**.**

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

**7 Click **OK**.**

## Adding a location with a wizard

You can add a group's location by using a wizard or when editing information about a group's location. Each location typically has its own set of policies and settings.

If you add a location with the Add a Location wizard, you also assign the location to a specific group. You also specify the conditions under which a group's policies and settings are switched to a new location that has its own policies and settings.

**To add a location with a wizard**

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

You can add locations only to groups that do not inherit policies from the parent group.
- 4** On the Clients page, under Tasks, click **Add Location**.
- 5** In the Welcome to the Add Location Wizard panel, click **Next**.
- 6** In the Specify Location Name panel, type a name and description for the new location, and click **Next**.
- 7** In the Specify a Condition panel, select any of the following conditions under which a client switches from one location to another:

No specific condition

Select this option so that the client can choose this location if multiple locations are available.

IP address range

Select this option so that the client can choose this location if its IP address is included in the specified range. You must specify both the start IP address and end IP address.

Subnet address and subnet mask	Select this option so that the client can choose this location if its subnet mask and subnet address are specified.
DNS server	Select this option so that the client can choose this location if it connects to the specified DNS server.
Client can resolve host name	Select this option so that the client can choose this location if it connects to the specified domain name and DNS resolve address.
Client can connect to management server	Select this option so that the client can choose this location if it connects to the specified management server.
Network connection type	Select this option so that the client can choose this location if it connects to the specified type of networking connection. The client switches to this location when using any of the following connections: <ul style="list-style-type: none"><li>■ Any networking</li><li>■ Dial-up networking</li><li>■ Ethernet</li><li>■ Wireless</li><li>■ Check Point VPN-1</li><li>■ Cisco VPN</li><li>■ Microsoft PPTP VPN</li><li>■ Juniper NetScreen VPN</li><li>■ Nortel Contivity VPN</li><li>■ SafeNet SoftRemote VPN</li><li>■ Aventail SSL VPN</li><li>■ Juniper SSL VPN</li></ul>

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

## Adding a location without a wizard

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

See [“Adding a location with a wizard”](#) on page 315.

### To add a location without a wizard

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

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

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

## Assigning a default location

Every time you create a new group, the Symantec Endpoint Protection Manager console automatically creates a default location that is called Default. You can specify another location to be a default location.

### To assign a default location

- 1 In the Symantec Endpoint Protection Manager console, click **Clients**.
- 2 On the Clients page, under View Clients, click the group to which you want to assign a different default location.

- 3 On the Policies tab, uncheck **Inherit policies and settings from parent group "group name"**.
- 4 Under Tasks, click **Manage Locations**.
- 5 In the Manage Locations dialog box, under Locations, select the location that you want to be the default location.
- 6 Under Description, check **Set this location as the default location in case of conflict**.  
  
The Default location is always the default location until you assign another one to the group.
- 7 Click **OK**.

## Editing the name and description of a group's location

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

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

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

## Deleting a group's location

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

### To delete a location

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

You can delete locations only from the groups that do not inherit policies from their parent groups.

- 4 On the Clients page, under Tasks, click **Manage Locations**.
- 5 In the Manage Locations dialog box, under Locations, select the location that you want to delete, and then click **Delete**.

You cannot delete the location that is set as the default location.

- 6 In the Delete Condition dialog box, click **Yes**.





# Working with policies

This chapter includes the following topics:

- [About working with policies](#)
- [About adding policies](#)
- [About editing policies](#)
- [Editing a shared policy in the Policies page](#)
- [Editing a non-shared or shared policy in the Clients page](#)
- [Assigning a shared policy](#)
- [Withdrawing a policy](#)
- [Deleting a policy](#)
- [Exporting a policy](#)
- [Importing a policy](#)
- [About copying policies](#)
- [Copying a shared policy in the Policy page](#)
- [Copying a shared or non-shared policy in the Clients page](#)
- [Pasting a policy](#)
- [Replacing a policy](#)
- [Converting a shared policy to a non-shared policy](#)
- [Converting a copy of a shared policy to a non-shared policy](#)

## About working with policies

You can perform the following tasks on all of the policies:

- Add  
If you add or edit shared policies in the Policies page, you must also assign the policies to a group or location. Otherwise those policies are not effective.
- Edit
- Assign
- Delete
- Import and export
- Copy and paste
- Convert
- Replace

Each task, where applicable, has appropriate cross-references to tasks that describe the specific components of each type of policy.

These policies can be either a shared policy or a non-shared policy.

## About adding policies

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

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

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

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

See [“Adding a shared policy in the Policies page”](#) on page 323.

See [“Adding a non-shared policy in the Clients page with a wizard”](#) on page 324.

## Adding a shared policy in the Policies page

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

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

See [“Adding a non-shared policy in the Clients page with a wizard”](#) on page 324.

### To add a shared policy in the Policies page

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

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

- 7 To configure the policy, under View Policies, click any of the following types of policies:

Antivirus and Antispyware	See <a href="#">“About working with Application and Device Control Policies”</a> on page 502.
Firewall	See <a href="#">“About working with Firewall Policies”</a> on page 426.
Intrusion Prevention	See <a href="#">“About working with Intrusion Prevention Policies”</a> on page 450.
Application and Device Control	See <a href="#">“About working with Application and Device Control Policies”</a> on page 502.
Host Integrity	See <a href="#">“About working with Host Integrity Policies”</a> on page 548.
LiveUpdate	See <a href="#">“About LiveUpdate and updating definitions and content”</a> on page 85.
Centralized Exceptions	See <a href="#">“About working with Centralized Exceptions Policies”</a> on page 532.

- 8 When you are done with the configuration of the policy, click **OK**.
- 9 In the Assign Policy dialog box, do one of the following tasks:
  - To assign the policy to a group or location now, click **Yes**, and then go to step 10.
  - To assign the policy to a group or a location later, click **No**.  
See [“Assigning a shared policy”](#) on page 329.

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

## Adding a non-shared policy in the Clients page with a wizard

You can add non-shared or shared policies in the Clients page.

You can add a shared policy in the Policies page

See [“Adding a shared policy in the Policies page”](#) on page 323.

**To add a non-shared policy in the Clients page with a wizard**

- 1 In the console, click **Policies**.
- 2 On the Policies page, under View Policies, locate the group to which you want to add the 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 add a policy.

- 4 Under Location-specific Policies and Settings, scroll down to the location.
- 5 To the right of Location-specific Policies, click **Add a policy**.

If a shared or location-specific policy already exists, it no longer appears in the Add Policy for *location name* wizard.

- 6 In the Add Policy for *location name* wizard, select the policy type that you want to add, and then click **Next**.

You can add location-specific policies only if none exists. Add a policy only appears if no policy exists for a specific type of policy.

- 7 Select from the following choices:

Use an existing shared policy	Creates a non-shared policy from a shared policy of the same type. If you edit this policy, it changes in all the locations that use this policy.  See <a href="#">“Adding a new non-shared policy from an existing policy in the Clients page”</a> on page 326.
Create a new policy	Creates a non-shared policy.  See <a href="#">“Adding a new non-shared policy in the Clients page”</a> on page 326.
Import a policy from a policy file	Creates a non-shared policy from a .dat formatted file that was previously exported.  See <a href="#">“Adding a new non-shared policy from a previously exported policy file in the Clients page”</a> on page 327.

## Adding a new non-shared policy in the Clients page

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

See [“Adding a non-shared policy in the Clients page with a wizard”](#) on page 324.

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

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

Antivirus and Antispyware	See <a href="#">“About working with Antivirus and Antispyware Policies”</a> on page 359.
Firewall	See <a href="#">“About working with Firewall Policies”</a> on page 426.
Intrusion Prevention	See <a href="#">“About working with Intrusion Prevention Policies”</a> on page 450.
Application and Device Control	See <a href="#">“About working with Application and Device Control Policies”</a> on page 502.
Host Integrity	See <a href="#">“About working with Host Integrity Policies”</a> on page 548.
LiveUpdate	See <a href="#">“About LiveUpdate and updating definitions and content”</a> on page 85.
Centralized Exceptions	See <a href="#">“About working with Centralized Exceptions Policies”</a> on page 532.

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

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

See [“Adding a non-shared policy in the Clients page with a wizard”](#) on page 324.

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

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

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

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

See [“Adding a non-shared policy in the Clients page with a wizard”](#) on page 324.

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

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

## About editing policies

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

## Editing a shared policy in the Policies page

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

**To edit a shared policy in the Policies page**

- 1 In the Symantec Endpoint Protection Manager console, click **Policies**.
- 2 On the Policies page, under View Policies, click the policy type.

- 3 In the *policy type* Policies pane, click the specific policy that you want to edit
- 4 Under Tasks, click **Edit the Policy**.
- 5 In the *policy type* Policy Overview pane, edit the name and description of the policy, if necessary.
- 6 To edit the policy, click any of the *policy type* Policy pages for the following policies:

Antivirus and Antispyware	See <a href="#">“About working with Antivirus and Antispyware Policies”</a> on page 359.
Firewall	See <a href="#">“About working with Firewall Policies”</a> on page 426.
Intrusion Prevention	See <a href="#">“About working with Intrusion Prevention Policies”</a> on page 450.
Application and Device Control	See <a href="#">“About working with Application and Device Control Policies”</a> on page 502.
Host Integrity	See <a href="#">“About working with Host Integrity Policies”</a> on page 548.
LiveUpdate	See <a href="#">“About LiveUpdate and updating definitions and content”</a> on page 85.
Centralized Exceptions	See <a href="#">“About working with Centralized Exceptions Policies”</a> on page 532.

## Editing a non-shared or shared policy in the Clients page

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

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

- 1 In the Symantec Endpoint Protection Manager console, click **Clients**.
- 2 On the Clients page, under View Clients, select the group for which you want to 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:

Antivirus and Antispyware	See <a href="#">“About working with Antivirus and Antispyware Policies”</a> on page 359.
Firewall	See <a href="#">“About working with Firewall Policies”</a> on page 426.
Intrusion Prevention	See <a href="#">“About working with Intrusion Prevention Policies”</a> on page 450.
Application and Device Control	See <a href="#">“About working with Application and Device Control Policies”</a> on page 502.
Host Integrity	See <a href="#">“About working with Host Integrity Policies”</a> on page 548.
LiveUpdate	See <a href="#">“About LiveUpdate and updating definitions and content”</a> on page 85.
Centralized Exceptions	See <a href="#">“About working with Centralized Exceptions Policies”</a> on page 532.

## Assigning a shared policy

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

#### To assign a shared policy

- 1 Add a shared policy.  
See [“Adding a shared policy in the Policies page”](#) on page 323.
- 2 On the Policies page, under View Policies, select the policy type that you want to assign.
- 3 In the *policy type* Policies pane, select the specific policy that you want to assign
- 4 On the Policies page, under Tasks, click **Assign the Policy**.
- 5 In the Assign *policy type* Policy dialog box, check the groups and locations to which you want to assign the policy.
- 6 Click **Assign**.
- 7 Click **Yes** to confirm that you want to assign the policy.

## Withdrawing a policy

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

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

- Antivirus and Antispyware
- LiveUpdate

---

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

---

#### To withdraw a shared policy in the Policies page

- 1 In the Symantec Endpoint Protection Manager console, click **Policies**.
- 2 On the Policies page, under View Policies, click the type of policy that you want to withdraw.
- 3 In the *policy type* Policies pane, click the specific policy that you want to withdraw.
- 4 On the Policies page, under Tasks, click **Withdraw the Policy**.

- 5 In the Withdraw Policy dialog box, check the groups and locations from which you want to withdraw the policy.
- 6 Click **Withdraw**.
- 7 When you are prompted to confirm the withdrawal of the policy from the groups and locations, click **Yes**.

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

- 1 In the Symantec Endpoint Protection Manager console, click **Clients**.
- 2 On the Clients page, under View Clients, select the group for which you want to withdraw a policy.
- 3 On the Policies tab, uncheck **Inherit policies and settings from parent group "group name"**.  
You must disable inheritance for this group. If you do not uncheck inheritance, you cannot withdraw a policy.
- 4 Under Location-specific Policies and Settings, scroll to find the name of the location for which you want to withdraw a policy.
- 5 Locate the policy for the location that you want to withdraw.
- 6 Click **Tasks**, and then click **Withdraw Policy**.
- 7 In the Withdraw Policy dialog box, click **Yes**.

## Deleting a policy

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

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

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

---

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

---

### To delete a shared policy in the Policy page

- 1 In the Symantec Endpoint Protection Manager console, click **Policies**.
- 2 In the Policies page, under View Policies, select the type of policy that you want to delete.  
  
The policy may or may not have been assigned to one or more groups and one or more locations.
- 3 In the *policy type* Policies pane, click the specific policy that you want to delete.
- 4 In the Policies page, under Tasks, click **Delete the Policy**.
- 5 When you are prompted to confirm that you want to delete the policy that you selected, click **Yes**.

### To delete a non-shared policy in the Clients page

- 1 In the Symantec Endpoint Protection Manager console, click **Clients**.
- 2 In the Clients page, under View Clients, select the group for which you want to delete a policy.
- 3 On the Policies tab, uncheck **Inherit policies and settings from parent group "group name"**.  
  
You must disable inheritance for this group. If you do not uncheck inheritance, you cannot delete a policy.
- 4 Under Location-specific Policies and Settings, scroll to find the name of the location whose policy you want to delete.
- 5 Locate the specific policy for the location that you want to delete.
- 6 To the right of the selected policy, click **Tasks**, and then click **Withdraw Policy**.  
  
When you withdraw the policy, you delete it at the same time. You cannot delete an Antivirus and Antispyware Policy or a LiveUpdate Policy from a location. You can only replace it with another policy.
- 7 Click **Yes**.

## Exporting a policy

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

You can export a shared or non-shared policy.

#### To export a shared policy in the Policies page

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

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

- 1 In the Symantec Endpoint Protection Manager console, click **Clients**.
- 2 On the Clients page, under View Clients, select the group for which you want to export a policy.
- 3 On the Policies tab, uncheck **Inherit policies and settings from parent group "group name"**.  
You must disable inheritance for this group. If you do not uncheck inheritance, you cannot export a policy.
- 4 Under Location-specific Policies and Settings, scroll to find the name of the location whose policy you want to export.
- 5 Locate the specific policy for the location that you want to export.
- 6 To the right of the policy, click **Tasks**, and then click **Export Policy**.
- 7 In the Export Policy dialog box, browse for the folder into which you want to export the policy.
- 8 In the Export Policy dialog box, click **Export**.

## Importing a policy

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

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

See [“Adding a new non-shared policy from a previously exported policy file in the Clients page”](#) on page 327.

#### To import a shared policy in the Policies page

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

## About copying policies

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

See “[Pasting a policy](#)” on page 335.

## Copying a shared policy in the Policy page

You can copy a shared policy in the Policy page.

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

See “[Copying a shared or non-shared policy in the Clients page](#)” on page 335.

#### To copy a shared policy in the Policy page

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

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

- 6 Click **OK**.

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

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

You can also copy shared policies in the Policy page.

See [“Copying a shared policy in the Policy page”](#) on page 334.

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

- 1 In the Symantec Endpoint Protection Manager console, click **Clients**.
- 2 On the Clients page, under View Clients, select the group for which you want to 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 In the Copy Policy dialog, check **Do not show this message again**.  
You check this option only if you no longer want to be notified about this process. The message states that the policy has been copied to the clipboard and is ready to be pasted.
- 7 Click **OK**.

# Pasting a policy

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

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

See [“About copying policies”](#) on page 334.

## To paste a shared policy in the Policy page

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

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

- 1 In the Symantec Endpoint Protection Manager console, click **Clients**.
- 2 On the Clients page, under View Clients, select the group for which you want to paste a policy.
- 3 On the Policies tab, uncheck **Inherit policies and settings from parent group "group name"**.  
You must disable inheritance for this group. If you do not uncheck inheritance, you cannot paste a policy.
- 4 Under Location-specific Policies and Settings, scroll to find the name of the location whose policy you want to paste.
- 5 Locate the specific policy for the location that you want to paste.
- 6 To the right of the policy, click **Tasks**, and then click **Paste**.
- 7 When you are prompted to overwrite the existing policy, click **Yes**.

## Replacing a policy

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

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

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

### To replace a shared policy for all locations

- 1 In the Symantec Endpoint Protection Manager console, click **Policies**.
- 2 On the Policies page, under View Policies, click the type of policy that you want to replace.
- 3 In the *policy type* Policies pane, click the policy.
- 4 In the Policies page, under Tasks, click **Replace the Policy**.
- 5 In the Replace *policy type* Policy dialog box, in the New *policy type* Policy drop-down list, select the shared policy that replaces the old one.
- 6 Select the groups and locations for which you want to replace the existing policy.



- 7 Click **Replace**.
- 8 When you are prompted to confirm the replacement of the policy for the groups and locations, click **Yes**.

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

- 1 In the console, click **Clients**.
- 2 In the Clients page, under View Clients, select the group for which you want to replace a policy.
- 3 On the Policies tab, uncheck **Inherit policies and settings from parent group "group name"**.  
You must disable inheritance for this group. If you do not uncheck inheritance, you cannot replace a policy.
- 4 Under Location-specific Policies and Settings, scroll to find the location that contains the policy.
- 5 Next to the policy that you want to replace, click **Tasks**, and then click **Replace Policy**.
- 6 In the Replace Policy dialog box, in the New policy drop-down list, select the replacement policy.
- 7 Click **OK**.

## Converting a shared policy to a non-shared policy

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

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

#### To convert a shared policy to a non-shared policy

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

If you do not uncheck inheritance, you cannot export any policies.

- 5 Under Location-specific Policies and Settings, scroll to find the name of the location whose policy you want to convert.
- 6 Locate the specific policy for the location that you want to convert.
- 7 Click **Tasks**, and then click **Convert to Non-shared Policy**.
- 8 In the Overview dialog box, edit the name and description of the policy.
- 9 Click **OK**.

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

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

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

- 1 In the console, click **Clients**.
- 2 In the Clients page, under View Clients, select the group for which you want to replace a policy.
- 3 On the Policies tab, uncheck **Inherit policies and settings from parent group "group name"**.  
You must disable inheritance for this group. If you do not uncheck inheritance, you cannot replace a policy.
- 4 Under Location-specific Policies and Settings, scroll to find the location that contains the policy.
- 5 Next to the policy that you want to replace, click **Tasks**, and then click **Edit Policy**.
- 6 In the Edit Policy dialog box, click **Create Non-Shared Policy From Copy**.
- 7 Edit the policy.  
See [“About editing policies”](#) on page 327.
- 8 When you are done with the configuration of the policy, click **OK**.

# Pushing and pulling policies between management servers, clients, and optional Enforcers

This chapter includes the following topics:

- [About pull mode and push mode](#)
- [Specifying push or pull mode](#)

## About pull mode and push mode

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

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

## About the heartbeat

A heartbeat is the frequency at which client computers upload data and download policies. A heartbeat is a protocol that each client uses to communicate with the Symantec Endpoint Protection Manager. The heartbeat frequency is a key factor in the number of clients that each Symantec Endpoint Protection Manager can support. Symantec Corporation recommends the following for large deployments. Deployments of 1,000 seats or more should set the heartbeat frequency to the maximum length of time that meets a company's security requirements.

For example, if you want to update security policies and gather logs on a daily basis, then set the heartbeat frequency to 24 hours. This setting enables each client to communicate with Symantec Endpoint Protection Manager shortly after you restart Symantec Endpoint Protection Manager. The first time a heartbeat occurs is based on the heartbeat frequency that you set. This first heartbeat occurrence is calculated as follows:

*heartbeat frequency* x .05 (5%)

When you set a heartbeat frequency to 30 minutes, the first heartbeat occurs in 90 seconds. This interval is calculated as 5 percent of the heartbeat setting. 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. You might have a requirement for a high heartbeat frequency in a large deployment (1000 seats or more) on each Symantec Endpoint Protection Manager. In this case, consult Symantec Professional Services and Symantec Enterprise Support to assess the proper configuration, hardware, and network architecture necessary for your network environment.

## Specifying push or pull mode

You can specify whether the management server pushes the policy down to the clients or that the clients pull the policy from the management server. The push mode is the default. If you select the pull mode, you must also set the frequency that each client connects to the management server. You can set the push or pull mode for groups or locations.

### To specify push or pull mode for a group

- 1 In the console, click **Clients**.
- 2 On the Clients page, under View Clients, select the group for which you want to specify whether to push or pull policies.
- 3 On the Clients page, click the **Policies** tab.

- 4 On the Policies tab, uncheck **Inherit policies and setting from the parent group "group name"**.
- 5 Under Location-independent Policies and Settings pane, under Settings, click **Communications Settings**.
- 6 In the Communications Settings for *group name* dialog box, under Download, verify that **Download policies and content from the management server** is checked.
- 7 Do one of the following tasks:
  - Click **Push mode**.
  - Click **Pull mode** and under Heartbeat Interval, set the number of minutes or hours.
- 8 Click **OK**.

#### To specify push or pull mode for a location

- 1 In the console, click **Clients**.
- 2 On the Clients page, under View Clients, select the group for which you want to specify whether to push or pull policies.
- 3 On the Clients page, click the **Policies** tab.
- 4 On the Policies tab, uncheck **Inherit policies and setting from the parent group "Global"**.
- 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 > Edit Settings**, 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**.

342 | Pushing and pulling policies between management servers, clients, and optional Enforcers  
| **Specifying push or pull mode**

# Setting up learned applications

This chapter includes the following topics:

- [About learned applications](#)
- [Enabling learned applications](#)
- [Searching for applications](#)

## About learned applications

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

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

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

The console includes a query tool for you to search for a list of applications. 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.

---

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

---

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

---

## Enabling learned applications

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

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

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

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

See [“Creating administrator notifications”](#) on page 195.

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



### To enable learned applications for a site

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

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

---

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

---

### To send the learned applications list to the management server

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

### To send learned applications to the management server for a location

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

Checking this setting enables you to create a location setting rather than a group setting.

- 5 Click **Tasks**, and then click **Edit Settings**.

- 6 In the Communications Settings for *location name* dialog box, check **Learn applications that run on the client computers**.
- 7 Click **OK**.

## Searching for applications

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

You can search for an application in the following ways:

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

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

See [“Adding applications to a rule”](#) on page 472.

The information about the clients that you can choose from in the Search Field is collected from the clients when you add client.

See [“Viewing a client's properties”](#) on page 63.

### To search for applications

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

You can specify only one group at a time.

- 5 Make sure that **Search subgroups** is checked.
- 6 Do one of the following actions:

- To search by user or computer information, click **Based on client/computer information**.
  - To search by application, click **Based on applications**.
- 7 Click the empty cell under **Search Field**, and then select the search criterion from the list.

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

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

If you enter more than one row of search criteria, the query tries to match all conditions.
  - 11 Click **Search**.
  - 12 In the Query Results table, do any of the following tasks:
    - Click the scroll arrows to view additional rows and columns.
    - Click **Previous** and **Next** to see additional screens of information.
    - Select a row, and then click **View Details** to see additional information about the application.

The results are not saved unless you export them to a file.
  - 13 To remove the query results, click **Clear All**.
  - 14 Click **Close**.

## Saving the results of an application search

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

### To save the results of an application search

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

See “[Searching for applications](#)” on page 346.
- 2 In the Search for Applications dialog box, under Query Results, click **Export**.

- 3 In the Export Results dialog box, type the number for the page that contains the application details and client computer details that you want to export.
- 4 Select or type the path name and the file name where you want to export the file, and then click **Export**.
- 5 To confirm, click **OK**.
- 6 If you are finished searching for applications, click **Close**.

# Configuring Antivirus and Antispyware Protection

- [Basic Antivirus and Antispyware Policy settings](#)
- [Configuring Auto-Protect](#)
- [Using administrator-defined scans](#)



# Basic Antivirus and Antispyware Policy settings

This chapter includes the following topics:

- [Basics of Antivirus and Antispyware Protection](#)
- [About working with Antivirus and Antispyware Policies](#)
- [About viruses and security risks](#)
- [About scanning](#)
- [About actions for the viruses and the security risks that scans detect](#)
- [Setting up log handling parameters in an Antivirus and Antispyware Policy](#)
- [About client interaction with antivirus and antispyware options](#)
- [Changing the password that is required to scan mapped network drives](#)
- [Specifying how Windows Security Center interacts with the Symantec Endpoint Protection client](#)
- [Displaying a warning when definitions are out of date or missing](#)
- [Specifying a URL to appear in antivirus and antispyware error notifications](#)
- [Specifying a URL for a browser home page](#)
- [Configuring the options that apply to antivirus and antispyware scans](#)
- [Submitting information about scans to Symantec](#)
- [Managing quarantined files](#)

# Basics of Antivirus and Antispyware Protection

You can provide Antivirus and Antispyware Protection for computers in your security network by doing the following actions:

- Create a plan to respond to viruses and security risks.
- View the status of your network on the Home page in the console.
- Run commands from the console to turn on Auto-Protect, launch an on-demand scan, or update definitions.
- Use Antivirus and Antispyware Policies to modify Auto-Protect and scan settings on client computers.

## About creating a plan to respond to viruses and security risks

An effective response to a virus and security risk outbreak requires a plan that lets you respond quickly and efficiently. You should create an outbreak plan and define actions to handle suspicious files.

[Table 29-1](#) outlines the tasks for creating a virus and security risk outbreak plan.

**Table 29-1** A sample plan

Task	Description
Ensure that definitions files are current.	Verify that infected computers have the latest definitions files. You can run reports to check that client computers have the latest definitions.  To update definitions, do any of the following actions: <ul style="list-style-type: none"><li>■ Apply a LiveUpdate policy. See <a href="#">“Configuring LiveUpdate Policies”</a> on page 92.</li><li>■ Run the Update Content command for a group or the selected computers that are listed on the Clients tab.</li><li>■ Run the Update Content command on the selected computers that are listed in a computer status or risk log.</li></ul>



**Table 29-1** A sample plan (*continued*)

Task	Description
Map your network topology.	<p>Prepare a network topology map so that you can systematically isolate and clean computers by segment before you reconnect them to your local network.</p> <p>Your map should contain the following information:</p> <ul style="list-style-type: none"> <li>■ Client computer names and addresses</li> <li>■ Network protocols</li> <li>■ Shared resources</li> </ul>
Understand security solutions.	<p>You should understand your network topology and your implementation of the client in your network. You should also understand the implementation of any other security products that are used on your network.</p> <p>Consider the following questions:</p> <ul style="list-style-type: none"> <li>■ What security programs protect network servers and workstations?</li> <li>■ What is the schedule for updating definitions?</li> <li>■ What alternative methods to obtain updates are available if the normal channels are under attack?</li> <li>■ What log files are available to track viruses on your network?</li> </ul>
Have a backup plan.	<p>In the event of a catastrophic infection, you may need to restore client computers. Make sure that you have a backup plan in place to restore critical computers.</p>
Isolate the infected computers.	<p>Blended threats such as worms can travel by shared resources without user interaction. When you respond to an infection by a computer worm, it can be critical to isolate the infected computers by disconnecting them from the network.</p>
Identify the risk.	<p>The management console reports and logs are a good source of information about risks on your network. You can use the Symantec Security Response Virus Encyclopedia to learn more about a particular risk that you identify in reports or logs. In some cases, you might find additional instructions for handling the risk.</p>

**Table 29-1** A sample plan (*continued*)

Task	Description
Respond to unknown risks.	<p>You should look at the Symantec Security Response Web site for up-to-date information when the following situations are true:</p> <ul style="list-style-type: none"><li>■ You cannot identify a suspicious file by examining the logs and reports.</li><li>■ The latest virus definitions files do not clean the suspicious file.</li></ul> <p>On the Web site, you might find recent information about the suspicious file. Check the Latest Virus Threats and Security Advisories.</p> <p><a href="http://securityresponse.symantec.com">http://securityresponse.symantec.com</a></p>

### Where to go for more information

You can search the online Symantec Knowledge Base for more information. The Knowledge Base contains the detailed information that was not available at the time of the publication of this guide.

<http://securityresponse.symantec.com>

You can also check the Symantec Security Response Web page for up-to-date information about viruses and security risks.

[http://www.symantec.com/enterprise/security\\_response/](http://www.symantec.com/enterprise/security_response/)

## About viewing the antivirus and antispyware status of your network

You can quickly view the status of your security network on the Home page in the console. A status summary shows you how many computers in your security network have disabled Antivirus and Antispyware Protection. An action summary shows the actions that the client performed on the detected viruses and security risks. The Home page also includes the virus definitions distribution across the network.

See “Using the Symantec Endpoint Protection Home page” on page 128.

You can also run reports and view logs.

See “About using Monitors and Reports to help secure your network” on page 201.

## About running commands for Antivirus and Antispyware Protection

You can quickly run commands from the Clients page in the console or by using the computer status logs from the Monitors page.

### About enabling Auto-Protect manually

The default Antivirus and Antispyware Policy enables Auto-Protect by default. If users on client computers disable Auto-Protect, you can quickly re-enable it in the console.

You can select the computers for which you want to enable Auto-Protect in the console on the Clients page. You can also enable Auto-Protect from a log that you generate from the Monitors page.

See [“Enabling File System Auto-Protect”](#) on page 396.

### About running on-demand scans

You can include scheduled scans as part of Antivirus and Antispyware Policies. However, you might need to manually run scans on client computers.

You can select computers for which you want to run on-demand scans in the console on the Clients page. You can also run an on-demand scan from a log that you generate from the Monitors page.

You can run an active, full, or custom scan. If you choose to run a custom scan, the client uses the settings for on-demand scans that you configure in the Antivirus and Antispyware Policy.

See [“Running on-demand scans”](#) on page 416.

## About Antivirus and Antispyware Policies

An Antivirus and Antispyware Policy includes the following types of options:

- Auto-Protect scans
- Administrator-defined scans (scheduled and on-demand scans)
- TruScan proactive threat scans
- Quarantine options
- Submissions options
- Miscellaneous parameters

When you install Symantec Endpoint Protection, several Antivirus and Antispyware policies appears in the policy list in the console. You can modify one of the preconfigured policies, or you can create new policies.

---

**Note:** Antivirus and Antispyware Policies include configuration for TruScan proactive threat scans.

See [“About scanning”](#) on page 363.

---

## About the preconfigured Antivirus and Antispyware Policies

The following preconfigured Antivirus and Antispyware Policies are available:

- Antivirus and Antispyware Policy
- Antivirus and Antispyware Policy - High Performance
- Antivirus and Antispyware Policy - High Security

The High Security Policy is the most stringent of all the preconfigured Antivirus and Antispyware Policies. You should be aware that it can affect the performance of other applications.

The High Performance Policy provides better performance than the High Security Policy, but it does not provide the same safeguards. It relies primarily on File System Auto-Protect to scan files with selected file extensions to detect threats.

The default Antivirus and Antispyware Policy contains the following important settings:

- File System Auto-Protect loads at computer startup and is enabled for all files.
- Internet Email, Microsoft Outlook, and Lotus Notes Auto-Protect are enabled for all files.
- File System Auto-Protect network scanning is enabled.
- TruScan proactive threat scans are enabled, and run once every hour.
- ActiveScan does not run automatically when new definitions arrive.
- A scheduled scan runs once per week, with scan tuning set to Best Application Performance.

The High Performance Policy contains the following important settings:

- File System Auto-Protect loads when Symantec Endpoint Protection starts and is enabled for files with selected extensions.
- File System Auto-Protect network scanning is disabled.
- Internet Email, Microsoft Outlook, and Lotus Notes Auto-Protect are disabled.
- Proactive threat scans are enabled, and run once every 6 hours.
- ActiveScan does not run automatically when new definitions arrive.

- A scheduled scan runs once a month with scan tuning set to Best Application Performance.

The High Security Policy contains the following important settings:

- File System Auto-Protect loads at computer startup and is enabled for all files.
- Internet Email, Microsoft Outlook, and Lotus Notes Auto-Protect are enabled for all files.
- File System Auto-Protect network scanning is enabled.
- Proactive threat scans are enabled and run once every hour, as well as every time a new process starts.
- ActiveScan runs automatically when new definitions arrive.
- A scheduled scan runs once per week, with scan tuning set to Balanced.

## About locking settings in Antivirus and Antispyware Policies

You can lock some settings in an Antivirus and Antispyware Policy. When you lock settings, users cannot change the settings on the client computers that use the policy.

## About Antivirus and Antispyware Policies for legacy clients

If your environment contains multiple versions of legacy clients, your Antivirus and Antispyware Policy might contain the settings that cannot be applied. You might need to configure and manage separate Antivirus and Antispyware Policies for legacy clients.

## About default settings for handling suspicious files

Using the default Antivirus and Antispyware Policy, the Symantec Endpoint Protection client performs the following actions when it identifies a file that it suspects a virus infected:

- The client tries to repair the file.
- If the file cannot be repaired with the current set of definitions, the client moves the infected file to the local Quarantine. In addition, the client makes a log entry of the risk event. The client forwards the data to the management server. You can view the log data from the console.

You can perform the following additional actions to complete your virus handling strategy:

- Configure the reports feature to notify you when viruses are found. See [“Using notifications”](#) on page 193.

- Define the different repair actions that are based on the virus type. For example, you can configure the client to fix macro viruses automatically. Then you can configure a different action for the client to take when it detects a program file.
- Assign a backup action for the files that the client cannot repair.  
See [“Configuring actions for known virus and security risk detections”](#) on page 384.
- Configure the local Quarantine to forward infected files to a Central Quarantine Server. You can configure the Central Quarantine to try a repair. When the Central Quarantine tries a repair, it uses its set of virus definitions. The Central Quarantine definitions might be more up to date than the definitions on the local computer. You can also automatically forward samples of infected files to Symantec Security Response for analysis.  
For more information, see the *Symantec Central Quarantine Administrator's Guide*.

## About using policies to manage items in the Quarantine

When the client detects a known virus, it places the file in the client computer's local Quarantine. The client might also quarantine the items that proactive threat scans detect. You configure the Quarantine settings as part of an Antivirus and Antispyware Policy that you apply to clients.

You can specify the following:

- A local Quarantine directory path
- Whether clients manually submit quarantined items to Symantec Security Response
- Whether clients automatically submit quarantined items to a Central Quarantine Server
- How the local Quarantine handles remediation when new virus definitions arrive

See [“Managing quarantined files”](#) on page 390.

You can also delete quarantined items on your client computers from the Risk log in the console.

See [“About using Monitors and Reports to help secure your network”](#) on page 201.

# About working with Antivirus and Antispyware Policies

You create and edit Antivirus and Antispyware Policies similarly to how you create and modify other types of policies. You can assign, withdraw, replace, copy, export, import, or delete an Antivirus and Antispyware Policy.

You typically assign a policy to multiple groups in your security network. You can create a non-shared, location-specific policy if you have specific requirements for a particular location.

The procedures in this chapter assume that you are familiar with the basics of policy configuration.

See [“About working with policies”](#) on page 322.

## About viruses and security risks

An Antivirus and Antispyware Policy scans for both viruses and for security risks; examples of security risks are spyware, adware, and other files that can put a computer or a network at risk. Antivirus and antispyware scans detect kernel-level rootkits. Rootkits are the programs that try to hide themselves from a computer's operating system and can be used for malicious purposes.

The default Antivirus and Antispyware Policy does the following actions:

- Detects, removes, and repairs the side effects of viruses, worms, Trojan horses, and blended threats.
- Detects, removes, and repairs the side effects of security risks such as adware, dialers, hacking tools, joke programs, remote access programs, spyware, trackware, and others.

[Table 29-2](#) describes the types of risks for which the client software scans.

**Table 29-2** Viruses and security risks

Risk	Description
Viruses	<p>Programs or code that attach a copy of themselves to another computer program or document when it runs. When the infected program runs, the attached virus program activates and attaches itself to other programs and documents. When a user opens a document that contains a macro virus, the attached virus program activates and attaches itself to other programs and documents.</p> <p>Viruses generally deliver a payload, such as displaying a message on a particular date. Some viruses specifically damage data. These viruses can corrupt programs, delete files, or reformat disks.</p>
Malicious Internet bots	<p>Programs that run automated tasks over the Internet for malicious purposes.</p> <p>Bots can be used to automate attacks on computers or to collect information from Web sites.</p>
Worms	<p>Programs that replicate without infecting other programs. Some worms spread by copying themselves from disk to disk, while others replicate only in memory to slow a computer down.</p>
Trojan horses	<p>Malicious programs that hide themselves in something benign, such as a game or utility.</p>
Blended threats	<p>Threats that blend the characteristics of viruses, worms, Trojan horses, and code with server and Internet vulnerabilities to initiate, transmit, and spread an attack. Blended threats use multiple methods and techniques to spread rapidly and cause widespread damage throughout the network.</p>



**Table 29-2** Viruses and security risks (*continued*)

Risk	Description
Adware	<p>Stand-alone or appended programs that secretly gather personal information through the Internet and relay it back to another computer. Adware may track browsing habits for advertising purposes. Adware can also deliver advertising content.</p> <p>Adware can be unknowingly downloaded from Web sites, typically in shareware or freeware, or can arrive through email messages or instant messenger programs. Often a user unknowingly downloads adware by accepting an End User License Agreement from a software program.</p>
Dialers	<p>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.</p>
Hacking tools	<p>Programs that are used by a hacker to gain unauthorized access to a user's computer. For example, one hacking tool is a keystroke logger, which tracks and records individual keystrokes and sends this information back to the hacker. The hacker can then perform port scans or vulnerability scans. Hacking tools may also be used to create viruses.</p>
Joke programs	<p>Programs that alter or interrupt the operation of a computer in a way that is intended to be humorous or frightening. For example, a program can be downloaded from a Web site, email message, or instant messenger program. It can move the Recycle Bin away from the mouse when the user tries to delete it or cause the mouse to click in reverse.</p>
Other	<p>Other security risks that do not conform to the strict definitions of viruses, Trojan horses, worms, or other security risk categories.</p>

**Table 29-2** Viruses and security risks (*continued*)

Risk	Description
Remote access programs	<p>Programs that allow access over the Internet from another computer so that they can gain information or attack or alter a user's computer. For example, a user may install a program, or another process might install a program without the user's knowledge. The program can be used for malicious purposes with or without modification of the original remote access program.</p>
Spyware	<p>Stand-alone programs that can secretly monitor system activity and detect passwords and other confidential information and relay it back to another computer.</p> <p>Spyware can be unknowingly downloaded from Web sites, typically in shareware or freeware, or can arrive through email messages or instant messenger programs. Often a user unknowingly downloads spyware by accepting an End User License Agreement from a software program.</p>
Trackware	<p>Stand-alone or appended applications that trace a user's path on the Internet and send information to the target system. For example, the application can be downloaded from a Web site, email message, or instant messenger program. It can then obtain confidential information regarding user behavior.</p>

By default, Auto-Protect scans for viruses, Trojan horses, worms, and security risks when it runs.

Some risks, such as Back Orifice, were detected as viruses in earlier versions of the client software. They remain detected as viruses so that the client software can continue to provide protection for legacy computers.

## About scanning

You can include the following types of scans in an Antivirus and Antispyware Policy:

- Antivirus and antispyware scans
  - Auto-Protect scans
  - Administrator-defined scans
- TruScan proactive threat scans

By default, all antivirus and antispyware scans detect viruses and security risks, such as adware and spyware; the scans quarantine the viruses and the security risks, and then they remove or repair their side effects. Auto-Protect and administrator-defined scans detect known viruses and security risks. Proactive threat scans detect unknown viruses and security risks by scanning for potentially malicious behavior.

---

**Note:** Sometimes, you might unknowingly install an application that includes a security risk such as adware or spyware. If Symantec determines that blocking the risk does not harm the computer, the client software blocks the risk. If blocking the risk might leave the computer in an unstable state, the client waits until the application installation is complete before it quarantines the risk. It then repairs the risk's side effects.

---

## About Auto-Protect scans

Auto-Protect scans include the following types of scans:

- File System Auto-Protect scans
- Auto-Protect email attachment scans for Lotus Notes and Outlook (MAPI and Internet)
- Auto-Protect scans for the Internet email messages and the attachments that use the POP3 or SMTP communications protocols; Auto-Protect scans for Internet email also include outbound email heuristics scanning

---

**Note:** For performance reasons, Internet Email Auto-Protect for POP3 is not supported on server operating systems. On a Microsoft Exchange server, you should not install Microsoft Outlook Auto-Protect.

---

Auto-Protect continuously scans files and email data for viruses and for security risks; viruses and security risks can include spyware and adware, as they are read from or written to a computer.

You can configure Auto-Protect to scan only selected file extensions. When it scans selected extensions, Auto-Protect can also determine a file's type even if a virus changes the file's extension.

When you configure Auto-Protect settings, you can lock Auto-Protect options on clients to enforce a company security policy for viruses and security risks. Users cannot change the options that you lock.

Auto-Protect is enabled by default. You can view Auto-Protect status in the console under the Clients tab or by generating the reports and the logs that show computer status. You can also view Auto-Protect status directly on the client.

Auto-Protect scans can scan email attachments for the following applications:

- Lotus Notes 4.5x, 4.6, 5.0, and 6.x
- Microsoft Outlook 98/2000/2002/2003/2007 (MAPI and Internet)

If you use Microsoft Outlook over MAPI or Microsoft Exchange client and you have Auto-Protect enabled for email, attachments are immediately downloaded to the computer that is running the email client. The attachments are scanned when the user opens the message. If you download a large attachment over a slow connection, mail performance is affected. You may want to disable this feature for users who regularly receive large attachments.

---

**Note:** If Lotus Notes or Microsoft Outlook is already installed on the computer when you perform a client software installation, the client software detects the email application. The client then installs the correct Auto-Protect plug-in. Both plug-ins are installed if you select a complete installation when you perform a manual installation.

---

If your email program is not one of the supported data formats, you can protect your network by enabling Auto-Protect on your file system. If a user receives a message with an infected attachment on a Novell GroupWise Email system, Auto-Protect can detect the virus when the user opens the attachment. This outcome is because most email programs save attachments to a temporary directory when users launch attachments from the email program. If you enable Auto-Protect on your file system, Auto-Protect detects the virus as it is written to the temporary directory. Auto-Protect also detects the virus if the user tries to save the infected attachment to a local drive or network drive.

## About Auto-Protect detection of the processes that continuously download the same security risk

If Auto-Protect detects a process that continuously downloads a security risk to a client computer, Auto-Protect can display a notification and log the detection. (Auto-Protect must be configured to send notifications.) If the process continues to download the same security risk, multiple notifications appear on the user's computer, and Auto-Protect logs multiple events. To prevent multiple notifications and logged events, Auto-Protect automatically stops sending notifications about the security risk after three detections. Auto-Protect also stops logging the event after three detections.

In some situations, Auto-Protect does not stop sending notifications and logging events for the security risk.

Auto-Protect continues to send notifications and log events when any of the following is true:

- You or users on client computers disable blocking the installation of security risks (the default is enabled).
- The action for the type of security risk that the process downloads has an action of Leave alone.

## About the automatic exclusion of files and folders

The client software automatically detects the presence of certain third-party applications and Symantec products. After it detects them, it creates exclusions for these files and folders. The client excludes these files and folders from all antivirus and antispyware scans.

The client software automatically creates exclusions for the following items:

- Microsoft Exchange
- Active Directory domain controller
- Certain Symantec products

---

**Note:** To see the exclusions that the client creates on 32-bit computers, you can examine the contents of the HKEY\_LOCAL\_MACHINE\Software\Symantec\Symantec Endpoint Protection\AV\Exclusions registry. You must not edit this registry directly. On 64-bit computers, look in HKEY\_LOCAL\_MACHINE\Software\Wow6432Node\Symantec\Symantec Endpoint Protection\AV\Exclusions.

---

The client does not exclude the system temporary folders from scans because doing so can create a significant security vulnerability on a computer.

You can configure any additional exclusions by using centralized exceptions.

For information about using centralized exceptions, see [“Configuring a Centralized Exceptions Policy”](#) on page 534.

### **About the automatic exclusion of files and folders for Microsoft Exchange server**

If Microsoft Exchange servers are installed on the computer where you installed the Symantec Endpoint Protection client, the client software automatically detects the presence of Microsoft Exchange. When the client software detects a Microsoft Exchange server, it creates the appropriate file and folder exclusions for File System Auto-Protect and all other scans. Microsoft Exchange servers can include clustered servers. The client software checks for changes in the location of the appropriate Microsoft Exchange files and folders at regular intervals. If you install Microsoft Exchange on a computer where the client software is already installed, the exclusions are created when the client checks for changes. The client excludes both files and folders; if a single file is moved from an excluded folder, the file remains excluded.

The client software creates file and folder scan exclusions for the following Microsoft Exchange server versions:

- Exchange 5.5
- Exchange 6.0
- Exchange 2000
- Exchange 2003
- Exchange 2007
- Exchange 2007 SP1

For Exchange 2007, see your user documentation for information about compatibility with antivirus software. In a few circumstances, you might need to create scan exclusions for some Exchange 2007 folders manually. For example, in a clustered environment, you might need to create some exclusions.

For more information, see "Preventing Symantec Endpoint Protection 11.0 from scanning the Microsoft Exchange 2007 directory structure" in the Symantec Knowledge Base at the following URL:

<http://service1.symantec.com/SUPPORT/ent-security.nsf/docid/2007072619121148>

### About the automatic exclusion of files and folders from Symantec products

The client creates appropriate file and folder scan exclusions for certain Symantec products when they are detected.

The client creates exclusions for the following Symantec products:

- Symantec Mail Security 4.0, 4.5, 4.6, 5.0, and 6.0 for Microsoft Exchange
- Symantec AntiVirus/Filtering 3.0 for Microsoft Exchange
- Norton AntiVirus 2.x for Microsoft Exchange
- Symantec Endpoint Protection Manager embedded database and logs

### About the automatic exclusion of Active Directory files and folders

The client software creates file and folder exclusions for the Active Directory domain controller database, logs, and working files. The client monitors the applications that are installed on the client computer. If the software detects Active Directory on the client computer, the software automatically creates the exclusions.

### If client email applications use a single inbox

The applications that store all email in a single file include Outlook Express, Eudora, Mozilla, and Netscape. If your client computers use any email applications that use a single inbox, you should create a centralized exception to exclude the Inbox file. The exception applies to all antivirus and antispyware scans as well as Auto-Protect.

The Symantec Endpoint Protection client quarantines the entire Inbox and users cannot access their email if the following statements are true:

- The client detects a virus in the Inbox file during an on-demand or scheduled scan.
- The action that is configured for the virus is Quarantine.

Symantec does not usually recommend excluding files from scans. When you exclude the Inbox file from scans, the Inbox cannot be quarantined; however, if the client detects a virus when a user opens an email message, it can safely quarantine or delete the message.

## About administrator-defined scans

Administrator-defined scans are the antivirus and antispyware scans that detect known viruses and security risks. For the most complete protection, you should schedule occasional scans for your client computers. Unlike Auto-Protect, which scans files and email as they are read to and from the computer,

administrator-defined scans detect viruses and security risks.

Administrator-defined scans detect viruses and security risks by examining all files and processes (or a subset of files and processes). Administrator-defined scans can also scan memory and loadpoints.

You configure administrator-defined scans as part of an Antivirus and Antispyware Policy.

Administrator-defined scans include the following types of scans:

- Scheduled scans
- On-demand scans

Typically, you might want to create a full scheduled scan to run once a week, and an Active Scan to run once per day. By default, Symantec Endpoint Protection client generates an Active Scan to run at startup on client computers.

## About scheduled scans

You can schedule scans to run at certain times. Users can also schedule scans for their computers from client computers, but they cannot change or disable the scans that you schedule for their computers. The client software runs one scheduled scan at a time. If more than one scan is scheduled at the same time, they run sequentially.

Scheduled scans have settings that are similarly to Auto-Protect scan settings, but each type of scan is configured separately. Centralized exceptions that you configure apply to all types of antivirus and antispyware scans.

If a computer is turned off during a scheduled scan, the scan does not run unless the computer is configured to run missed scan events.

Scheduled scans inspect files for viruses and security risks, such as spyware and adware.

[Table 29-3](#) describes the types of scheduled scans.

**Table 29-3** Types of scheduled scans

Type	Description
Active Scan	Scans the system memory and all the common virus and security risk locations on the computer quickly. The scan includes all processes that run in memory, important registry files, and files like config.sys and windows.ini. It also includes some critical operating system folders.
Full Scan	Scans the entire computer for viruses and security risks, including the boot sector and system memory.



**Table 29-3** Types of scheduled scans (*continued*)

Type	Description
Custom Scan	Scans the files and folders that you select for viruses and security risks.

## About on-demand scans

You can run an on-demand scan from the console to inspect selected files and folders on selected client computers. On-demand scans provide immediate results from a scan on an area of the network or a local hard drive. You can run these scans from the Client tab in the console. You can also run these scans from the Monitors tab in the console.

See [“Running on-demand scans”](#) on page 416.

See [“Running commands and actions from logs”](#) on page 186.

The default on-demand scan scans all files and folders. You can change the settings for on-demand scans in an Antivirus and Antispyware Policy. In the policy, you can specify the file extensions and folders that you want to scan. When you run an on-demand scan from the Monitors page, the scan runs on the client based on the settings that are configured in the policy.

See [“Configuring on-demand scan options”](#) on page 415.

## About TruScan proactive threat scans

TruScan proactive threat scans use heuristics to scan for the behavior that is similar to virus and security risk behavior. Unlike antivirus and antispyware scans, which detect known viruses and security risks, Proactive threat scans detect unknown virus and security risks.

---

**Note:** Because proactive threat scanning examines active processes on client computers, the scanning can impact system performance.

---

The client software runs proactive threat scans by default. You can enable or disable proactive threat scanning in an Antivirus and Antispyware Policy. Users on client computers can enable or disable this type of scan if you do not lock the setting.

Although you include settings for proactive threat scans in an Antivirus and Antispyware Policy, you configure the scan settings differently from antivirus and antispyware scans.

See [“About TruScan proactive threat scans”](#) on page 481.

## About scanning after updating definitions files

If Auto-Protect is enabled, the client software begins scanning with the updated definitions files immediately.

When definitions files are updated, the client software tries to repair the files that are stored in Quarantine and scans active processes.

For proactive threat scan the detections that are quarantined, the files are scanned to see if they are now considered a virus or security risk. The client scans items quarantined by proactive threat scans similar to how it scans items quarantined by other types of scans. For quarantined detections, the client software completes the remediation and cleans up any side effects. If the proactive threat detection is now part of the Symantec white list, the client software restores and removes the detection from the quarantine; however, the process is not relaunched.

## About scanning selected extensions or folders

For each type of antivirus and antispyware scan and Auto-Protect, you can select files to include by extension. For administrator-defined scans, you can also select files to include by folder. For example, you can specify that a scheduled scan only scans certain extensions and that Auto-Protect scans all extensions.

When you select file extensions or folders for scans, you can select multiple extensions or the folders that you want to scan. Any extensions or folders that you do not select are excluded from the scan.

In the File Extensions dialog box, you can quickly add extensions for all common programs or all common documents. You can also add your own extensions. When you add your own extension, you can specify an extension with up to four characters.

In the Edit Folders dialog box, you select Windows folders, rather than absolute folder paths. Client computers in your security network might use different paths to these folders. You can select any of the following folders:

- COMMON\_APPDATA
- COMMON\_DESKTOPDIRECTORY
- COMMON\_DOCUMENTS
- COMMON\_PROGRAMS
- COMMON\_STARTUP
- PROGRAM\_FILES
- PROGRAM\_FILES\_COMMON
- SYSTEM

## ■ WINDOWS

When you scan selected file extensions or folders, you can improve scan performance. For example, if you copy a large folder that is not in the selected folders list, the copying process is faster because the folder's contents are excluded.

You can exclude files from scans by extension or directory type. You exclude files by configuring a Centralized Exceptions Policy that contains the exclusions. When you specify exclusions in a policy, the exclusions are applied any time any antivirus and antispyware scans run on clients with that policy.

See [“Configuring a Centralized Exceptions Policy”](#) on page 534.

When you scan selected extensions, the client software does not read the file header to determine the file type. When you scan selected extensions, the client scans only the files with the extensions that you specify.

---

**Warning:** Because the client software excludes files and folders from scans, it does not protect excluded files and folders from viruses and security risks.

---

[Table 29-4](#) describes the recommended extensions for scanning.

**Table 29-4** Recommended file extensions for scanning

File extension	Description
386	Driver
ACM	Driver; audio compression manager
ACV	Driver; audio compression or decompression manager
ADT	ADT file; fax
AX	AX file
BAT	Batch
BTM	Batch
BIN	Binary
CLA	Java Class
COM	Executable
CPL	Applet Control Panel for Microsoft Windows
CSC	Corel Script

**Table 29-4** Recommended file extensions for scanning (*continued*)

File extension	Description
DLL	Dynamic Link Library
DOC	Microsoft Word
DOT	Microsoft Word
DRV	Driver
EXE	Executable
HLP	Help file
HTA	HTML application
HTM	HTML
HTML	HTML
HTT	HTML
INF	Installation script
INI	Initialization file
JPEG	Graphics file
JPG	Graphics file
JS	JavaScript
JSE	JavaScript Encoded
JTD	Ichitaro
MDB	Microsoft Access
MP?	Microsoft Project
MSO	Microsoft Office 2000
OBD	Microsoft Office binder
OBT	Microsoft Office binder
OCX	Microsoft object that links and embeds custom control
OV?	Overlay
PIF	Program information file

**Table 29-4** Recommended file extensions for scanning (*continued*)

File extension	Description
PL	PERL program source code (UNIX)
PM	Presentation Manager Bitmaps Graphics
POT	Microsoft PowerPoint
PPT	Microsoft PowerPoint
PPS	Microsoft PowerPoint
RTF	Rich Text Format document
SCR	Fax, screensaver, snapshot, or script for Farview or Microsoft Windows
SH	Shell Script (UNIX)
SHB	Corel Show Background file
SHS	Shell scrap file
SMM	Lotus AmiPro
SYS	Device driver
VBE	VESA BIOS (Core Functions)
VBS	VBScript
VSD	Microsoft Office Visio
VSS	Microsoft Office Visio
VST	Microsoft Office Visio
VXD	Virtual device driver
WSF	Windows Script File
WSH	Windows Script Host Settings File
XL?	Microsoft Excel

## About excluding named files and folders

There might be certain security risks that your company's security policy lets you keep on your computers. You can configure the client to exclude these risks from all antivirus and antispyware scans.

You can exclude named files and folders from Auto-Protect and administrator-defined scans. For example, you can exclude the path C:\Temp\Install or folders that contain an allowable security risk. You can exclude the files that trigger false-positive alerts. For example, if you used another virus scanning program to clean an infected file, the program might not completely remove the virus code. The file may be harmless but the disabled virus code might cause the client software to register a false positive. Check with Symantec Technical Support if you are not sure if a file is infected.

When you create an exclusion, it applies to all types of antivirus and antispyware scans that you run. You create an exclusion as part of a centralized exception.

See [“Configuring a Centralized Exceptions Policy”](#) on page 534.

## About actions for the viruses and the security risks that scans detect

Many of the same scan options are available for different types of scans. When you configure on-demand, scheduled, or Auto-Protect scans, you can assign first and second actions to take when the client software finds viruses and security risks.

You can assign individual first and second actions to take when the client discovers the following types of risks:

- Macro viruses
- Non-macro viruses
- All security risks (adware, spyware, joke programs, dialers, hacking tools, remote access programs, trackware, and others)
- Individual categories of security risks, such as spyware
- Custom actions for a particular instance of a security risk

By default, the Symantec Endpoint Protection client first tries to clean a file that is infected by a virus.

If the client software cannot clean the file, it does the following actions:

- Moves the file to the Quarantine on the infected computer
- Denies access to the file
- Logs the event

By default, the client moves any files infected by security risks to the Quarantine on the infected computer. The client also tries to remove or repair the risk's side effects. By default, the Quarantine contains a record of all actions that the client

performed. If needed, the computer can be returned to the state that existed before the client tried the removal and repair.

If it is not possible to quarantine and repair a security risk, the second action is to log the risk.

For TruScan proactive threat scan detections, the actions are determined depending on whether you use Symantec-managed defaults or if you choose to set the actions yourself. You configure actions for proactive threat scans in a separate part of the Antivirus and Antispyware Policy.

See [“Specifying the actions and sensitivity levels for detecting Trojan horses, worms, and keyloggers”](#) on page 491.

## Setting up log handling parameters in an Antivirus and Antispyware Policy

You can include log handling parameters in the Antivirus and Antispyware Policy. By default, clients always send certain types of events to the management server (such as Scan stopped or Scan started). You can choose to send or not send other types of events (such as File not scanned).

The events that clients send to the management server affect information in reports and logs. You should decide what type of information that you want to forward to the management server. You can reduce the size of the logs and the amount of information included in reports if you select only certain types of events.

You can also configure how long the client retains log items. The option does not affect any events that the clients send to the management console. You can use the option to reduce the actual log size on the client computers.

You can click Help for more information about the options that are used in this procedure.

### To set up log handling parameters for an Antivirus and Antispyware Policy

- 1 On the Antivirus and Antispyware Policy page, click **Miscellaneous**.
- 2 On the Log Handling tab, under Antivirus and Antispyware Log Event Filtering, select the events that you want to forward to the management server.
- 3 Under Log Retention, select how often the client deletes log lines.
- 4 Under Log Event Aggregation, select how often aggregated events are sent to the server.
- 5 If you are finished with the configuration for this policy, click **OK**.

## About client interaction with antivirus and antispyware options

You can configure the specific parameters in the policy that control the client user experience.

You can do any of the following actions:

- Configure scan progress options for scheduled scans.
- Set scanning options for clients.
- Change the password that is required to scan mapped drives.
- Specify how Windows Security Center interacts with the Symantec Endpoint Security client.
- Display a warning when definitions are out of date or missing.
- Specify a URL to appear in antivirus and antispyware error notifications.
- Specify a URL to redirect an Internet browser if a security risk tries to change the URL.

You can display and customize warning messages on infected computers. For example, if users have a spyware program installed on their computers, you can notify them that they have violated your corporate policy. You can include a message in the notification that users must uninstall the application immediately.

---

**Note:** You can also lock policy settings so that users cannot change the settings.

---

## Changing the password that is required to scan mapped network drives

Symantec Endpoint Protection requires users on client computers to provide a password before they can scan a mapped network drive. By default, this password is set to symantec.

---

**Note:** If users scan network drives, the scan can impact the client computer performance.

---

You can click Help for more information about the options that are used in the procedure.



### To change the password that is required to scan mapped drives

- 1 On the Antivirus and Antispyware Policy page, click **Miscellaneous**.
- 2 On the Miscellaneous tab, under Scan Network Drive, check **Ask for password before scanning a mapped network drive**.
- 3 Click **Change Password**.
- 4 In the Configure Password dialog box, type a new password, and then confirm by typing the password again.
- 5 Click **OK**.
- 6 If you are finished with the configuration for this policy, click **OK**.

## Specifying how Windows Security Center interacts with the Symantec Endpoint Protection client

If you use Windows Security Center on Windows XP Service Pack 2 or Windows Vista, you can use the Antivirus and Antispyware Policy to set the following options on client computers:

- The time period after which Windows Security Center considers definitions files to be out of date.
- Whether Windows Security Center displays antivirus alerts for Symantec products on the host computer.

---

**Note:** Symantec product status is always available in the management console, regardless of whether Windows Security Center is enabled or disabled.

---

## Configuring the Symantec Endpoint Protection client to disable Windows Security Center

You can configure the circumstances under which the client software disables Windows Security Center.

### To configure Symantec Endpoint Protection to disable Windows Security Center

- 1 On the Antivirus and Antispyware Policy page, click **Miscellaneous**.
- 2 Click the **Miscellaneous** tab.

**Specifying how Windows Security Center interacts with the Symantec Endpoint Protection client**

- 3 Under Windows Security Center, in the Disable Windows Security Center drop-down list, select one of the following options:

Never	Never disable Windows Security Center.
Once	Disable Windows Security Center only once. If a user re-enables it, the client software does not disable it again.
Always	Always disable Windows Security Center. If a user re-enables it, the client software disables it again immediately.
Restore	Re-enable Windows Security Center only if Symantec Endpoint Protection disabled it.

- 4 Click **OK**.

## Configuring Symantec Endpoint Protection alerts to appear on the host computer

You can configure Windows Security Center to display alerts from the Symantec Endpoint Protection client.

### To configure alerts to appear on the host computer

- 1 On the Antivirus and Antispyware Policy page, click **Miscellaneous**.
- 2 Click the **Miscellaneous** tab.
- 3 Under Windows Security Center, in the Display Antivirus alerts within Windows Security Center drop-down menu, select one of the following options:

Disable	Windows Security Center does not display these alerts in the Windows notification area.
Enable	Windows Security Center displays these alerts on the Windows notification area.
Use existing setting	Windows Security Center uses the existing setting to display these alerts.

- 4 Click **OK**.

## Configuring the out-of-date time for definitions

By default, Windows Security Center considers Symantec definitions to be out of date after 30 days. You can change the number of days that definitions can be out

of date during installation in the Windows installer. You can also change the setting in the Antivirus and Antispyware Policy.

On client computers, the Symantec Endpoint Protection client checks every 15 minutes to compare the out-of-date time, the date of the definitions, and the current date. Typically, no out-of-date status is reported to Windows Security Center because definitions are usually updated automatically. If you update definitions manually you might have to wait up to 15 minutes to view an accurate status in Windows Security Center.

#### To configure the out-of-date time for definitions

- 1 On the Antivirus and Antispyware Policy page, click **Miscellaneous**.
- 2 Click the **Miscellaneous** tab.
- 3 Under Windows Security Center, under Display Windows Security Center message when definitions are outdated, type the number of days. You can also use the up or down arrow to select the number of days that the virus and security risk definitions can be out of date.  
The value must be in the range 1 to 30.
- 4 If you are finished with the configuration for this policy, click **OK**.

## Displaying a warning when definitions are out of date or missing

You can display and customize warning messages to appear on client computers when their virus and security risk definitions are outdated or missing. You might want to alert users if you do not have automatic updates scheduled. You also might want to alert users if you allow them to turn off LiveUpdate.

#### To display a warning about definitions

- 1 On the Antivirus and Antispyware Policy page, click **Miscellaneous**.
- 2 On the Notifications tab, under Actions, select one or both of the following options:
  - Display message when definitions are outdated
  - Display message when Symantec Endpoint Protection is running without virus definitions
- 3 For outdated virus and security risk definitions, set the number of days that definitions can be outdated before the warning appears.

- 4 For missing virus and security risk definitions, set the number of remediation tries that Symantec Endpoint Protection must make before the warning appears.
- 5 Click **Warning** for each option that you checked, and then customize the default message.
- 6 In the warning dialog box, click **OK**.
- 7 If you are finished with the configuration for this policy, click **OK**.

## Specifying a URL to appear in antivirus and antispyware error notifications

In rare cases, users might see errors appear on client computers. For example, the client computer might encounter buffer overruns or decompression problems during scans.

You can specify a URL that points to the Symantec support Web site or to a custom URL. For example, you might have an internal Web site that you want to specify instead.

---

**Note:** The URL also appears in the system event log for the client computer on which the error occurs.

---

### To specify a URL to appear in antivirus and antispyware error notifications

- 1 On the Antivirus and Antispyware Policy page, click **Miscellaneous**.
- 2 On the Notifications tab, check **Display error messages with a URL to a solution**.
- 3 Select one of the following options:
  - **Display the URL to a Symantec Technical Support Knowledge Base article**
  - **Display a custom URL**
- 4 Click **Customize Error Message** if you want to customize the message.
- 5 Enter the custom text that you want to include, and then click **OK**.
- 6 If you are finished with the configuration for this policy, click **OK**.

## Specifying a URL for a browser home page

You can specify a URL to use as the home page when the Symantec Endpoint Protection client repairs a security risk that hijacked a browser home page.

### To specify a URL for a browser home page

- 1 On the Antivirus and Antispyware Policy page, click **Miscellaneous**.
- 2 On the Miscellaneous tab, under Internet Browser Protection, type the URL.
- 3 If you are finished with the configuration for this policy, click **OK**.

## Configuring the options that apply to antivirus and antispyware scans

Some scanning options are common to all antivirus and antispyware scans. Antivirus and antispyware scans include both Auto-Protect and administrator-defined scans.

The policy includes the following options:

- Configure scans of selected file extensions or folders
- Configure centralized exceptions for security risks
- Configure actions for known virus and security risk detections
- Manage notification messages on infected computers
- Customize and display notifications on infected computers
- Add warnings to infected email messages
- Notify senders of infected email messages
- Notify users of infected email messages

Information about actions and notifications for proactive threat scans is included in a separate section.

See [“Configuring notifications for TruScan proactive threat scans”](#) on page 494.

## Configuring scans of selected file extensions

The Symantec Endpoint Protection client may complete scans faster by scanning only files with selected extensions. Scans that scan only selected extensions offer less protection to computers; however, when you scan only selected extensions you can select the file types that viruses typically attack. When you scan selected

extensions, you can make scans more efficient and use less of the computer's resources.

You can configure the extensions to scan to balance the following requirements:

- The amount of protection that your network requires
- The amount of time and resources that are required to provide the protection

For example, you might want to scan only the files with the extensions that are likely to contain a virus or other risk. When you scan only certain extensions, you automatically exclude all files with other extensions from the scan. When you exclude files from scans, you decrease the amount of computer resources that are required to run the scan.

---

**Warning:** When you select extensions that you want to scan, any other extensions are not protected from viruses and security risks.

---

You can click Help for more information about the options that are used in the procedure.

#### To include only files with particular extensions for Auto-Protect or administrator-defined scans

- 1 On the Scan Details tab, under File types, click **Scan only selected extensions**.
- 2 Click **Select Extensions**.
- 3 In the File Extensions dialog box, you can do any of the following:
  - To add your own extensions, type the extension, and then click **Add**.
  - To remove any extensions, select the extensions, and then click **Remove**.
  - To return the list to its default setting, click **Use Defaults**.
  - To add all program extensions, click **Add Common Programs**.
  - To add all document extensions, click **Add Common Documents**.
- 4 If you are finished with the configuration for this policy, click **OK**.

## Configuring the scans of selected folders

You can configure selected folders for certain administrator-defined scans to scan. These administrator-defined scans include custom scheduled scans and on-demand scans. You cannot configure selected folders for Auto-Protect.

See [“About scanning selected extensions or folders”](#) on page 370.

You can click Help for more information about the options that are used in this procedure.

#### To configure the scans of selected folders

- 1 On the Antivirus and Antispyware Policy page, click **Administrator-defined Scan**.
- 2 On the Scans tab, do one of the following:
  - Click **Add**.
  - Under Scheduled scans, select an existing scan, and then click **Edit**.
  - Under Administrator On-demand Scan, click **Edit**.
- 3 On the Scan Details tab, in the Scan type drop-down list, click **Custom Scan**.  
On-demand scans are preset to Custom Scan.
- 4 Under Scanning, click **Edit Folders**.
- 5 In the Edit Folders dialog box, click **Scan selected folders**, and then in the folder list, check all the folders that you want this scan to scan.  
  
The Selected folders field shows all of your choices.
- 6 Click **OK** until you return to the Administrator-defined Scan page.
- 7 If you are finished with the configuration for this policy, click **OK**.

## About exceptions for security risks

If you want any security risks to remain on your network, you can ignore the security risks when they are detected on client computers.

If a user has configured custom actions for a security risk that you have specified to ignore, the user's custom actions are not used.

---

**Note:** When you add a security risk to the exceptions list, the Symantec Endpoint Protection client no longer logs any events that involve that security risk. You can configure the client to log the risk even if you include the risk in the exceptions list. Regardless of whether the risk is logged or not, users are not notified in any way when the risk is present on their computers.

---

You can use a Centralized Exceptions Policy to configure exceptions.

See [“Configuring a Centralized Exceptions Policy”](#) on page 534.

## Configuring actions for known virus and security risk detections

You use actions to specify how clients respond when an antivirus and antispyware scan detects a known virus or security risk. These actions apply to Auto-Protect and administrator-defined scans. You configure actions for proactive threat scans separately.

See [“About TruScan proactive threat scans”](#) on page 481.

Actions allow you to set how the client software responds when it detects a known virus or a security risk. You can assign a first action and, in case the first action is not possible, a second action. The Symantec Endpoint Protection client uses these actions when it discovers a virus or a security risk such as adware or spyware. Types of viruses and security risks are listed in the hierarchy.

You can click Help for more information about the options that are used in the procedures.

---

**Note:** For security risks, use the delete action with caution. In some cases, deleting security risks causes applications to lose functionality.

---

**Warning:** If you configure the client software to delete the files that security risks affect, it cannot restore the files.

To back up the files that security risks affect, configure the client software to quarantine them.

---

### To configure actions for known virus and security risk detections

- 1 On the Actions tab, under Detection, select a type of virus or security risk.  
By default, each security risk subcategory is automatically configured to use the actions that are set for the entire Security Risks category.
- 2 To configure a specific instance of a security risk category to use different actions, check **Override actions configured for Security risks**, and then set the actions for that category only.
- 3 Under Actions for, select the first and second actions that the client software takes when it detects that category of virus or security risk.

You can lock actions so that users cannot change the action on client computers that use this policy.

For security risks, use the delete action with caution. In some cases, deleting security risks causes applications to lose functionality.



- 4 Repeat step 3 for each category for which you want to set actions (viruses and security risks).
- 5 If you are finished with the configuration for this policy, click **OK**.

## About notification messages on infected computers

You can enable a custom notification message to appear on infected computers when an administrator-defined scan or Auto-Protect finds a virus or security risk. These notifications can alert users to review their recent activity on the client computer. For example, a user might download an application or view a Web page that results in a spyware infection.

---

**Note:** The language of the operating system on which you run the client might not be able to interpret some characters in virus names. If the operating system cannot interpret the characters, the characters appear as question marks in notifications. For example, some unicode virus names might contain double-byte characters. On computers that run the client on an English operating system, these characters appear as question marks.

---

For Auto-Protect scans of email, you can also configure the following options:

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

See [“Configuring notification options for Auto-Protect”](#) on page 404.

Notifications for proactive threat scan results are configured separately.

See [“Configuring notifications for TruScan proactive threat scans”](#) on page 494.

## Customizing and displaying notifications on infected computers

You can construct a custom message to appear on infected computers when a virus or a security risk is found. You can type directly in the message field to add or modify the text.

When you run a remote scan, you can notify the user of a problem by displaying a message on the infected computer's screen. You can customize the warning message by including information such as the name of the risk, the name of an infected file, and the status of the risk. A warning message might look like the following example:

Scan type: Scheduled Scan  
 Event: Risk Found  
 SecurityRiskName: Stoned-C  
 File: C:\Autoexec.bat  
 Location: C:  
 Computer: ACCTG-2  
 User: JSmith  
 Action taken: Cleaned

Table 29-5 describes the variable fields that are available for notifications.

**Table 29-5** Notification message variables

Field	Description
SecurityRiskName	The name of the virus or security risk that was found.
ActionTaken	The action that was taken in response to detecting the virus or security risk.  This action can be either the first action or second action that was configured.
Status	The state of the file: Infected, Not Infected, or Deleted.  This message variable is not used by default. To display this information, you must manually add this variable to the message.
Filename	The name of the file that the virus or the security risk has infected.
PathAndFilename	The complete path and name of the file that the virus or the security risk has infected.
Location	The drive on the computer on which the virus or security risk was located.
Computer	The name of the computer on which the virus or security risk was found.
User	The name of the user who was logged on when the virus or security risk occurred.
Event	The type of event, such as Risk Found.
LoggedBy	The type of scan that detected the virus or security risk.
DateFound	The date on which the virus or security risk was found.
StorageName	The affected area of the application (for example, File System Auto-Protect or Lotus Notes Auto-Protect).

**Table 29-5** Notification message variables (continued)

Field	Description
ActionDescription	A full description of the actions that were taken in response to the detection of the virus or the security risk.

**To display notification messages on infected computers**

- 1 On the Antivirus and Antispyware Policy page, do one of the following actions:
  - Click **Administrator-defined Scans**.
  - Click **File System Auto-Protect**.
  - Click **Internet Email Auto-Protect**.
  - Click **Microsoft Outlook Auto-Protect**.
  - Click **Lotus Notes Auto-Protect**.
- 2 If you selected Administrator-defined Scan, on the Scans tab, click **Add** or **Edit**.
- 3 On the Notifications tab, check **Display a notification message on the infected computer** and modify the body of the notification message.
- 4 Click **OK**.

## Submitting information about scans to Symantec

You can specify that information about proactive threat scan detections and information about Auto-Protect or scan detections are automatically sent to Symantec Security Response.

Information that clients submit helps Symantec determine if a detected threat is real. If Symantec determines the threat is real, Symantec can generate a signature to address the threat. The signature is included in an updated version of definitions. For TruScan proactive threat detections, Symantec can update its lists of allowed or disallowed processes.

When a client sends information about a process, the information includes the following items:

- The path to the executable
- The executable
- The internal state information
- The information about the file and the registry load points that refer to the threat

- The content version that the proactive threat scan used

Any personal information that can identify the client computer is not submitted.

Information about detection rates potentially helps Symantec refine virus definitions updates. Detection rates show the viruses and security risks that are detected most by customers. Symantec Security Response can remove the signatures that are not detected, and provide a segmented virus definition list for the customers who request it. Segmented lists increase antivirus and antispyware scan performance.

When a proactive threat scan makes a detection, the client software checks to see if information about the process has already been sent. If the information has been sent, the client does not send the information again.

---

**Note:** When proactive threat scans detect items on the commercial applications list, the information about these detections is not forwarded to Symantec Security Response.

---

When you enable submission for processes, items that are quarantined by proactive threat scans are updated. When the items are updated, the Quarantine window shows that the samples have been submitted to Symantec Security Response. The client software does not notify users and the management console does not give an indication when detections with other types of actions are submitted. Other types of actions include Log or Terminate.

You can submit Quarantine samples to Symantec.

See [“Submitting quarantined items to Symantec”](#) on page 393.

## About submissions throttling

Clients may or may not submit samples to Symantec depending on the following information:

- The date of the Submission Data Control file
- The percentage of the computers that are allowed to send submissions

Symantec publishes its Submission Control Data (SCD) file and includes it as part of a LiveUpdate package. Each Symantec product has its own SCD.

The file controls the following settings:

- How many submissions a client can submit in one day
- How long to wait before the client software retries submissions
- How many times to retry failed submissions

- Which IP address of the Symantec Security Response server receives the submission

If the SCD becomes out-of-date, then clients stop sending submissions. Symantec considers the SCD out-of-date when a client computer has not retrieved LiveUpdate content in 7 days.

If clients stop the transmission of the submissions, the client software does not collect the submission information and send it later. When clients start to transmit submissions again, they only send the information about the events that occur after the transmission restart.

Administrators can also configure the percentage of computers that are allowed to submit. Each client computer determines whether or not it should submit information. The client computer randomly selects a number from 1 to 100. If the number is less than or equal to the percentage that is set in that computer's policy, then the computer submits information. If the number is greater than the configured percentage, the computer does not submit information.

## Configuring submissions options

Submissions are enabled by default. You can enable or disable submissions in an Antivirus and Antispyware Policy on the Submissions tab.

You can click Help for more information about the options that are used in this procedure.

### To specify whether or not information is sent about processes detected by TruScan proactive threat scans

- 1 On the Antivirus and Antispyware Policy page, click **Submissions**.
- 2 Under TruScan Proactive Threat Scans, check or uncheck **Allow client computers to submit processes detected by scans**.
- 3 When you check this parameter, you can change the percentage of client computers that are allowed to submit information about processes.
- 4 If you enabled submissions, use the up arrow or down arrow to select the percentage or type the desired value in the text box.
- 5 If you are finished with the configuration for this policy, click **OK**.

To specify whether or not information is sent about Auto-Protect and manual scan detection rates

- 1 On the Antivirus and Antispyware Policy page, click **Submissions**.
- 2 Under Detection Rates, check or uncheck **Allow client computers to submit threat detection rates**.

When you check this parameter, you can change the percentage of client computers that are allowed to submit detection rates.

- 3 If you are finished with the configuration for this policy, click **OK**.

## Managing quarantined files

Managing quarantined files includes the following:

- Specifying a local quarantine directory
- Submitting quarantined items to Symantec
- Configuring actions to take when new definitions arrive

### About Quarantine settings

You use the Antivirus and Antispyware Policy to configure client Quarantine settings.

You manage Quarantine settings as an important part of your virus outbreak strategy.

### Specifying a local Quarantine directory

If you do not want to use the default quarantine directory to store quarantined files on client computers, you can specify a different local directory. You can use path expansion by using the percent sign when you type the path. For example, you can type %COMMON\_APPDATA%. Relative paths are not allowed.

The software supports the following expansion parameters:

%COMMON_APPDATA%	This path is typically C:\Documents and Settings\All Users\Application Data
%PROGRAM_FILES%	This path is typically C:\Program Files
%PROGRAM_FILES_COMMON%	This path is typically C:\Program Files\Common

%COMMON_PROGRAMS%	This path is typically C:\Documents and Settings\All Users\Start Menu\Programs
%COMMON_STARTUP%	This path is typically C:\Documents and Settings\All Users\Start Menu\Programs\Startup
%COMMON_DESKTOPDIRECTORY%	This path is typically C:\Documents and Settings\All Users\Desktop
%COMMON_DOCUMENT%	This path is typically C:\Documents and Settings\All Users\Documents
%SYSTEM%	This path is typically C:\Windows\System32
%WINDOWS%	This path is typically C:\Windows

#### To specify a local quarantine directory

- 1 On the Antivirus and Antispyware Policy page, click **Quarantine**.
- 2 On the Miscellaneous tab, under Local Quarantine Options, click **Specify Quarantine Directory**.
- 3 In the text box, type the name of a local directory on the client computers. You can use path expansion by using the percent sign when typing in the path. For example, you can type %COMMON\_APPDATA%, but relative paths are not allowed.
- 4 If you are finished with the configuration for this policy, click **OK**.

## Configuring automatic clean-up options

When the client software scans a suspicious file, it places the file in the local Quarantine folder on the infected computer. The Quarantine clean-up feature automatically deletes the files in the Quarantine when they exceed a specified age. The Quarantine clean-up feature automatically deletes the files in the Quarantine when the directory where they are stored reaches a certain size.

You can configure these options using the Antivirus and Antispyware Policy. You can individually configure the number of days to keep repaired, backup, and quarantined files. You can also set the maximum directory size that is allowed before files are automatically removed from the client computer.

You can use one of the settings, or you can use both together. If you set both types of limits, then all files older than the time you have set are purged first. If the size of the directory still exceeds the size limit that you set, then the oldest files are deleted one by one. The files are deleted until the directory size falls below the limit. By default, these options are not enabled.

### To configure automatic clean-up options

- 1 On the Antivirus and Antispyware Policy page, click **Quarantine**.
- 2 On the Cleanup tab, under Repaired files, check or uncheck **Enable automatic deleting of repaired files**.
- 3 In the Delete after box, type a value or click an arrow to select the time interval in days.
- 4 Check **Delete oldest files to fit directory size limit**, and then type in the maximum directory size, in megabytes. The default setting is 50 MB.
- 5 Under Backup files, check or uncheck **Enable automatic delete 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 fit directory size limit**, and then type the maximum directory size, in megabytes. The default is 50 MB.
- 8 Under Quarantined Files, check or uncheck **Enable automatic deleting of quarantined files that could not be repaired**.
- 9 In the Delete after box, type a value or click an arrow to select the time interval in days.
- 10 Check **Delete oldest files to fit directory size limit**, and then type in the maximum directory size, in megabytes. The default is 50 MB.
- 11 If you are finished with the configuration for this policy, click **OK**.

## Submitting quarantined items to a central Quarantine Server

You can enable items in Quarantine to be forwarded from the local Quarantine to a Central Quarantine Server. You should configure the client to forward items if you use a Central Quarantine Server in your security network. The Central Quarantine Server can forward the information to Symantec Security Response. Information that clients submit helps Symantec determine if a detected threat is real.

---

**Note:** Only the quarantined items that are detected by antivirus and antispyware scans may be sent to a Central Quarantine Server. Quarantined items that are detected by proactive threat scans cannot be sent.

---



### To enable submission of quarantined items to a Quarantine Server

- 1 On the Antivirus and Antispyware Policy page, click **Submissions**.
- 2 Under Quarantined Items, check **Allow client computers to automatically submit quarantined items to a Quarantine Server**.
- 3 Type the name of the Quarantine Server.
- 4 Type the port number to use, and then select the number of seconds to retry connecting.
- 5 If you are finished configuring settings for this policy, click **OK**.

## Submitting quarantined items to Symantec

You can enable the client software to allow users to submit infected or suspicious files and related side effects to Symantec Security Response for further analysis. When users submit information, Symantec can refine its detection and repair.

Files that are submitted to Symantec Security Response become the property of Symantec Corporation. In some cases, files may be shared with the antivirus community. If Symantec shares files, Symantec uses industry-standard encryption and may make data anonymous to help protect the integrity of the content and your privacy.

In some cases, Symantec might reject a file. For example, Symantec might reject a file because the file does not seem to be infected. You can enable the resubmission of files if you want users to be able to resubmit selected files. Users can resubmit files once per day.

### To enable submission of quarantined items to Symantec

- 1 On the Antivirus and Antispyware Policy page, click **Submissions**.
- 2 Under Quarantined Items, check **Allow client computers to manually submit quarantined items to Symantec Security Response**.
- 3 If you are finished with the configuration for this policy, click **OK**.

## Configuring actions to take when new definitions arrive

You can configure the actions that you want to take when new definitions arrive on client computers. By default, the client rescans items in the Quarantine and automatically repairs and restores items silently. Typically, you should always use this setting.

**To configure actions for new definitions**

- 1 On the Antivirus and Antispyware Policy page, click **Quarantine**.
- 2 On the General tab, under When new virus definitions arrive, click one of the following options:
  - **Automatically repair and restore files in Quarantine silently**
  - **Repair files in Quarantine silently without restoring**
  - **Prompt user**
  - **Do nothing**
- 3 If you are finished with the configuration for this policy, click **OK**.

# Configuring Auto-Protect

This chapter includes the following topics:

- [About configuring Auto-Protect](#)
- [About types of Auto-Protect](#)
- [Enabling File System Auto-Protect](#)
- [Configuring File System Auto-Protect](#)
- [Configuring Internet Email Auto-Protect](#)
- [Configuring Microsoft Outlook Auto-Protect](#)
- [Configuring Lotus Notes Auto-Protect](#)
- [Configuring notification options for Auto-Protect](#)

## About configuring Auto-Protect

You configure Auto-Protect settings as part of an Antivirus and Antispyware Policy. You can also manually enable Auto-Protect for a client group or particular computers and users.

You can lock or unlock many Auto-Protect options in an Antivirus and Antispyware Policy. When you lock an option, users on client computers cannot change the option. By default, options are unlocked.

Some options for Auto-Protect are similar to options for other antivirus and antispyware scans.

See [“Configuring the options that apply to antivirus and antispyware scans”](#) on page 381.

## About types of Auto-Protect

Auto-Protect protects both the file system and the email attachments that clients receive.

You can configure the following types of Auto-Protect:

- File System Auto-Protect
- Internet Email Auto-Protect
- Microsoft Outlook Auto-Protect
- Lotus Notes Auto-Protect

By default, all types of Auto-Protect are enabled. If your client computers run other email security products, such as Symantec Mail Security, you might not need to enable Auto-Protect for email.

See [“About Auto-Protect scans”](#) on page 363.

## Enabling File System Auto-Protect

Auto-Protect settings are included in the Antivirus and Antispyware Policy that you apply to the client computers. By default, File System Auto-Protect is enabled. You can lock the setting so that users on client computers cannot disable File System Auto-Protect. You might need to enable Auto-Protect from the console if you allow users to change the setting or if you disable File System Auto-Protect.

You can enable File System Auto-Protect by using the Clients tab in the console. You can also manually enable File System Auto-Protect from the computer status logs.

See [“Running commands and actions from logs”](#) on page 186.

If you want to disable Auto-Protect, you must disable the setting in the Antivirus and Antispyware Policy that is applied to the group.

### To enable File System Auto-Protect

- 1 In the console, click **Clients**, and then under View Clients, select the group that includes computers for which you want to enable Auto-Protect.
- 2 In the right pane, select the Clients tab.
- 3 Do one of the following actions:
  - In the left pane, under View Clients, right-click the group for which you want to enable Auto-Protect.
  - In the right pane, on the Clients tab, select the computers and users for which you want to enable Auto-Protect, and then right-click the selection.

- 4 Do one of the following actions:
  - Click **Run Command on Group > Enable Auto-Protect**
  - Click **Run Command on Clients > Enable Auto-Protect**
- 5 In the message that appears, click **OK**.

If you want to enable or disable Auto-Protect for email, you must include the setting in the Antivirus and Antispyware Policy.

## Configuring File System Auto-Protect

When you configure File System Auto-Protect as part of an Antivirus and Antispyware Policy, you configure the settings that define how Auto-Protect and its associated features behave. You specify whether you want to scan floppy disk drives, network drives, or both.

---

**Note:** When you configure Auto-Protect options, you can click the lock icon next to the Auto-Protect settings. Users with the client computers that use this policy cannot change the locked settings.

---

You can click Help for more information about the options that are used in the procedures.

### To configure File System Auto-Protect

- 1 On the Antivirus and Antispyware Policy page, click **File System Auto-Protect**.
- 2 On the Scan Details tab, check or uncheck **Enable File System Auto-Protect**.
- 3 Under Scanning, under File types, click one of the following options:
  - **Scan all files**
  - **Scan only selected extensions**

See “[Configuring scans of selected file extensions](#)” on page 381.
- 4 Under Additional options, check or uncheck **Scan for security risks** and **Block security risk from being installed**.

See “[About Auto-Protect security risk scanning and blocking](#)” on page 398.
- 5 Under Network Settings, check or uncheck **Network** to enable or disable Auto-Protect scans of network files.
- 6 If you checked Network, click **Network Settings**.
- 7 In the Network Settings dialog box, do any of the following actions:

- Enable or disable Auto-Protect to trust files on the remote computers that run Auto-Protect.
  - Configure network cache options for Auto-Protect scans.
- 8 Click **OK**.
  - 9 Under Floppy Settings, check or uncheck **Check floppies for boot viruses when accessed**.
  - 10 If you checked **Check floppies for boot viruses when accessed**, set the action you want to be taken when a boot virus is found, either to clean it from the boot record or to log it and leave it alone.
  - 11 On the Actions tab, set any of the options.  
See “[Configuring actions for known virus and security risk detections](#)” on page 384.
  - 12 On the Notifications tab, set any of the notification options.  
See “[Configuring notification options for Auto-Protect](#)” on page 404.
  - 13 On the Advanced tab, set any of the following options:
    - Startup and shutdown
    - Reload options
  - 14 Under Additional Options, click **File Cache** or **Risk Tracer**.
  - 15 Configure the file cache or Risk Tracer settings, and then click **OK**.
  - 16 If you are finished with the configuration for this policy, click **OK**.

## About Auto-Protect security risk scanning and blocking

By default, Auto-Protect does the following actions:

- Scans for security risks such as adware and spyware
- Quarantines the infected files
- Removes or repairs the side effects of the security risks

In cases where blocking the installation of a security risk does not affect the stability of a computer, Auto-Protect also blocks the installation by default. If Symantec determines that blocking a security risk could compromise a computer’s stability, then Auto-Protect allows the risk to install. Auto-Protect also immediately takes the action that is configured for the risk.

From time to time, however, you might temporarily need to disable scanning for security risks in Auto-Protect, and then enable it. You might also need to disable

blocking security risks to control the time at which Auto-Protect reacts to certain security risks.

---

**Note:** You cannot disable security risk scanning for other types of scans. However, you can configure Symantec Endpoint Protection to leave the security risk alone and log the detection. You can also exclude specific risks globally from all types of scans by adding them to the centralized exceptions list.

---

See [“About Centralized Exceptions Policies”](#) on page 531.

## Configuring advanced scanning and monitoring options

You can configure advanced scanning and monitoring options for Auto-Protect scans of files and processes. The options include when to scan files, and heuristic scanning settings.

Heuristic scanning as part of Auto-Protect is different from proactive threat scanning. Heuristic scanning as part of Auto-Protect scans files for malicious behavior, while proactive threat scanning inspects running processes for malicious behavior.

See [“About TruScan proactive threat scans”](#) on page 481.

You can click Help for more information about the options that are used in the procedures.

### To configure advanced scanning and monitoring options

- 1 On the Antivirus and Antispyware Policy page, click **File System Auto-Protect**.
- 2 On the Scan Details tab, under Scanning, click **Advanced Scanning and Monitoring**.
- 3 Under Scan Files When, specify what activities trigger scans.
- 4 Under Bloodhound(TM) Detection Settings, check or uncheck **Enable Bloodhound(TM) virus detection**.

You can also change the level of protection.

- 5 Click **OK**.
- 6 If you are finished with the configuration for this policy, click **OK**.

## About Risk Tracer

Risk Tracer identifies the source of network share-based virus infections on the computers that run Windows XP/2000/2003 operating systems.

When Auto-Protect detects an infection, it sends information to Rtvscan, the main Symantec Endpoint Protection service. Rtvscan determines if the infection originated locally or remotely.

If the infection came from a remote computer, Rtvscan can do the following actions:

- Look up and record the computer's NetBIOS computer name and its IP address.
- Look up and record who was logged on to the computer at delivery time.
- Display the information in the Risk properties dialog box.

Rtvscan polls every second by default for network sessions, and then caches this information as a remote computer secondary source list. This information maximizes the frequency with which Risk Tracer can successfully identify the infected remote computer. For example, a risk may close the network share before Rtvscan can record the network session. Risk Tracer then uses the secondary source list to try to identify the remote computer. You can configure this information in the Auto-Protect Advanced Options dialog box.

Risk Tracer information appears in the Risk Properties dialog box, and is available only for the risk entries that the infected files cause. When Risk Tracer determines that the local host activity caused an infection, it lists the source as the local host.

Risk Tracer lists a source as unknown when the following conditions are true:

- It cannot identify the remote computer.
- The authenticated user for a file share refers to multiple computers. This condition can occur when a user ID is associated with multiple network sessions. For example, multiple computers might be logged on to a file sharing server with the same server user ID.

You can record the full list of multiple remote computers that currently infect the local computer. Set the HKEY\_LOCAL\_MACHINE\Software\Symantec\Symantec Endpoint Protection\AV\ProductControl\Debug string value to "THREATTRACER X" on the local client computer. The THREATTRACER value turns on the debug output and the X ensures that only the debug output for Risk Tracer appears. You can also add an L to ensure that the logging goes to the <SAV\_Program\_Folder>\vpdebug.log log file. To ensure that the debug window does not appear, add XW.

If you want to experiment with this feature, use the test virus file Eicar.com available from the following URL:

[www.eicar.org](http://www.eicar.org)

Risk Tracer also includes an option to block the IP addresses of source computers. For this option to take effect, you must set the corresponding option in the firewall policy to enable this type of automatic blocking.



# Configuring Internet Email Auto-Protect

Internet Email Auto-Protect protects both incoming email messages and outgoing email messages that use the POP3 or SMTP communications protocol over the Secure Sockets Layer (SSL). When Internet Email Auto-Protect is enabled, the client software scans both the body text of the email and any attachments that are included.

You can enable Auto-Protect to support the handling of encrypted email over POP3 and SMTP connections. Auto-Protect detects the secure connections and does not scan the encrypted messages. Even if Internet Email Auto-Protect does not scan encrypted messages, it continues to protect computers from viruses and security risks in attachments.

File System Auto-Protect scans email attachments when you save the attachments to the hard drive.

---

**Note:** Internet Email Auto-Protect is not supported for 64-bit computers. Internet Email Auto-Protect also does not support scanning of POP3 email on server operating systems.

---

The Symantec Endpoint Protection client also provides outbound email heuristics scanning. The heuristics scanning uses Bloodhound Virus Detection to identify the risks that may be contained in outgoing messages. When the client scans outgoing email messages, the scan helps to prevent the spread of risks. These risks include the worms that can use email clients to replicate and distribute themselves across a network.

Email scanning does not support the following email clients:

- IMAP clients
- AOL clients
- HTTP-based email such as Hotmail and Yahoo! Mail

You can click Help for more information about the options that are used in the procedures.

## To configure Internet Email Auto-Protect

- 1 On the Antivirus and Antispyware Policy page, click **Internet Email Auto-Protect**.
- 2 On the Scan Details tab, check or uncheck **Enable Internet Email Auto-Protect**.
- 3 Under Scanning, under File types, click one of the following options:

- **Scan all files**
  - **Scan only selected extensions**  
See “[Configuring scans of selected file extensions](#)” on page 381.
- 4 Check or uncheck **Scan files inside compressed files**.
  - 5 Click **OK**.
  - 6 On the Actions tab, set any of the options.  
See “[Configuring actions for known virus and security risk detections](#)” on page 384.
  - 7 Click **OK**.
  - 8 On the Notifications tab, under Email Notifications, check or uncheck any of the following options:
    - **Insert a warning into the email message**
    - **Send email to the sender**
    - **Send email to others**See “[Configuring notification options for Auto-Protect](#)” on page 404.
  - 9 Click **OK**.
  - 10 On the Advanced tab, under Encrypted Connections, enable or disable encrypted POP3 or SMTP connections.
  - 11 Under Mass Mailing Worm Heuristics, check or uncheck **Outbound worm heuristics**.
  - 12 If you are finished with the configuration for this policy, click **OK**.

## Configuring Microsoft Outlook Auto-Protect

By default, Auto-Protect scans Microsoft Outlook email attachments. You can customize the scan settings.

You can click Help for more information about the options that are used in the procedures.

### To configure Microsoft Outlook Auto-Protect

- 1 On the Antivirus and Antispyware Policy page, click **Microsoft Outlook Auto-Protect**.
- 2 On the Scan Details tab, check or uncheck **Enable Microsoft Outlook Auto-Protect**.

- 3 Under Scanning, under File types, click one of the following options:
  - **Scan all files**
  - **Scan only selected extensions**See [“Configuring scans of selected file extensions”](#) on page 381.
- 4 Check or uncheck **Scan files inside compressed files**.
- 5 On the Actions tab, set any of the options.  
See [“Configuring actions for known virus and security risk detections”](#) on page 384.
- 6 On the Notifications tab, check or uncheck of the following options:
  - **Insert a warning into the email message**
  - **Send email to the sender**
  - **Send email to others**See [“Configuring notification options for Auto-Protect”](#) on page 404.
- 7 If you are finished with the configuration for this policy, click **OK**.

## Configuring Lotus Notes Auto-Protect

By default, Auto-Protect scans Lotus Notes email attachments. You can customize the scan settings.

You can click Help for more information about the options that are used in the procedures.

### To configure Lotus Notes Auto-Protect

- 1 On the Antivirus and Antispyware Policy page, click **Lotus Notes Auto-Protect**.
- 2 On the Scan Details tab, check or uncheck **Enable Lotus Notes Auto-Protect**.
- 3 Under Scanning, under File types, click one of the following options:
  - **Scan all files**
  - **Scan only selected extensions**See [“Configuring scans of selected file extensions”](#) on page 381.
- 4 Check or uncheck **Scan files inside compressed files**.
- 5 On the Actions tab, set any of the options.  
See [“Configuring actions for known virus and security risk detections”](#) on page 384.

- 6 On the Notifications tab, check or uncheck any of the following options:
  - **Insert a warning into the email message**
  - **Send email to the sender**
  - **Send email to others**See “[Configuring notification options for Auto-Protect](#)” on page 404.
- 7 If you are finished configuring policy settings, click **OK**.

## Configuring notification options for Auto-Protect

By default, the results of File System Auto-Protect scans appear on infected computers. You can configure the Antivirus and Antispyware Policy so that results do not appear on client computers.

You can customize the notification message that appears on client computers when Auto-Protect makes a detection.

See “[Customizing and displaying notifications on infected computers](#)” on page 385.

For supported email software, you can also configure Auto-Protect to do the following actions:

- Add a warning to email messages about infected computers.
- Notify senders of infected email messages.
- Notify others of infected email messages.

You can customize the email messages that you send to notify users.

---

**Note:** Use caution when you configure the options to notify senders and others about infected email messages. The address of the infected email message might be spoofed. If you send notifications, you might generate spam and cause increased traffic on your network.

---

The variable fields that you customize for notifications messages and email messages are slightly different. You can customize the information in the message body and the information in the infection field.

[Table 30-1](#) describes the email message body fields.

**Table 30-1** Email message body fields

Field	Description
User	The name of the user who was logged on when the virus or security risk occurred.
DateFound	The date on which the virus or security risk was found.
EmailSender	The email address that sent the email with the infected attachment.
EmailRecipientList	The list of addresses to which the email with the infected attachment was sent.

[Table 30-2](#) describes the infection information fields.

**Table 30-2** Infection information fields

Field	Description
SecurityRiskName	The name of the virus or security risk that was found.
ActionTaken	The action that was taken in response to detecting the virus or security risk. This action can be either the first action or the second action that was configured.
Status	The state of the file: Infected, Not Infected, or Deleted.  This message variable is not used by default. To display this information, manually add this variable to the message.
Filename	The name of the file that the virus or the security risk infected.
PathAndFilename	The complete path and name of the file that the virus or security risk infected.
Computer	The name of the computer on which the virus or security risk was found.
User	The name of the user who was logged on when the virus or security risk occurred.
DateFound	The date on which the virus or security risk was found.
OriginalAttachmentName	The name of the attachment that contains the virus or security risk.

**Table 30-2** Infection information fields (*continued*)

Field	Description
StorageName	The affected area of the application. For example, the storage name might be File System Auto-Protect or Lotus Notes Auto-Protect.

## Displaying Auto-Protect results on infected computers

If you want users to view the results of Auto-Protect scans of files and processes, you can display the results on the infected computers. You can also disable the display if you do not want the results to appear on client computers.

You can click Help for more information about the options that are used in the procedures.

### To display Auto-Protect results on infected computers

- 1 On the Antivirus and Antispyware Policy page, click **File System Auto-Protect**.
- 2 On the Notifications tab, check or uncheck **Display the Auto-Protect results dialog on the infected computer**.
- 3 If you are finished configuring policy settings, click **OK**.

## Adding warnings to infected email messages

For supported email software, you can configure Auto-Protect to insert a warning automatically into the body of an infected email message. A warning message is important if the Symantec Endpoint Protection client is unable to clean the virus from the message. The message is also important if an infected attachment file is moved, left alone, deleted, or renamed. The warning message tells you which virus was found and explains the action that was taken.

You can append the following text to the top of the email message that is associated with the infected attachment:

Symantec Endpoint Protection found a security risk in an attachment from [EmailSender].

For each infected file, the following information is also added to the email message:

- The name of the file attachment
- The name of the risk
- The action taken
- The infection status of the file

You can customize the subject and body of the message.

The email message contains a field called *EmailSender*. You can customize the default message.

The message would look as follows to the recipient:

```
Symantec Endpoint Protection found a security risk in an
attachment from John.Smith@mycompany.com.
```

You can click Help for more information about the options that are used in the procedures.

#### To add email warnings to infected email messages

- 1 On the Antivirus and Antispyware Policy page, do one of the following actions:
  - Click **Internet Email Auto-Protect**.
  - Click **Microsoft Outlook Auto-Protect**.
  - Click **Lotus Notes Auto-Protect**.
- 2 On the Notifications tab, under Email Notifications, check **Insert a warning into the email message**.
- 3 Click **Warning** and do one of the following actions:
  - Click **OK** to accept the default message.
  - Customize the warning message.
- 4 If you are finished with the configuration for this policy, click **OK**.

## Notifying senders of infected email messages

For supported email software, you can configure Auto-Protect to respond automatically to the sender of an email message that contains an infected attachment.

---

**Note:** Use caution when you configure the options to notify senders about infected email messages. The address of the infected email message might be spoofed. If you send notifications, you might generate spam and cause increased traffic on your network.

---

You can also configure Auto-Protect to send a default reply email message with the following subject:

Security risk found in message “[EmailSubject]”

The body of the message informs the sender of the infected attachment:

Symantec Endpoint Protection found a security risk in an attachment you ([EmailSender]) sent to [EmailRecipientList].

For each infected file, the following information is also added to the email message:

- The name of the file attachment
- The name of the risk
- The action taken
- The infection status of the file

You can also customize this message.

#### To notify senders of infected email messages

- 1 On the Antivirus and Antispyware Policy page, do one of the following actions:
  - Click **Internet Email Auto-Protect**.
  - Click **Microsoft Outlook Auto-Protect**.
  - Click **Lotus Notes Auto-Protect**.
- 2 On the Notifications tab, under Email Notifications, check **Send email to the sender**.
- 3 Click **Sender**.
- 4 In the Send Email to Sender dialog box, on the Message tab, under Message Text, do one of the following actions:
  - Click **OK** to accept the default message.
  - Type a subject line, message body, and infection information to appear in each message, and then click **OK**.  
You can click Help for information about the variables that you can use in the message.
- 5 For Internet Email Auto-Protect only, on the Email Server tab, type the following information:
  - The mail server name and port
  - The user name and password
  - The reverse path for the email
- 6 If you are finished with the configuration for this policy, click **OK**.

## Notifying others of infected email messages

For supported email software, you can configure Auto-Protect to notify others whenever an email message that contains an infected attachment is opened.



---

**Note:** Use caution when you configure the options to notify others about infected email messages. The address of the infected email message might be spoofed. If you send notifications, you might generate spam and cause increased traffic on your network.

---

You can send an email message to other users with the following subject:

Security risk found in message “[EmailSubject]”

The body of the message includes information about the sender of the infected attachment:

Symantec Endpoint Protection found a security risk in an attachment from [EmailSender].

For each infected file, the following information is also added to the email message:

- The name of the file attachment
- The name of the risk
- The action taken
- The infection status of the file

You can also customize this message.

#### To notify others of infected email messages

- 1 On the Antivirus and Antispyware Policy page, do one of the following actions:
  - Click **Internet Email Auto-Protect**.
  - Click **Microsoft Outlook Auto-Protect**.
  - Click **Lotus Notes Auto-Protect**.
- 2 On the Notifications tab, under Email Notifications, check **Send email to others**.
- 3 Click **Others**.
- 4 In the Send Email to Others dialog box, on the Others tab, provide one or more email addresses to which notifications should be sent.
- 5 Click the Message tab and type a subject line, message body, and infection information to appear in each message.

You can click Help for information about the variables that you can use in the message.

- 6 For Internet Email Auto-Protect only, on the Email Server tab, type the following information:.

- The mail server name and port
  - The user name and password
  - The reverse path for the email
- 7 Click **OK**.
  - 8 If you are finished with the configuration for this policy, click **OK**.

## Configuring progress notifications for Auto-Protect scans of Internet email

You can enable or disable progress indicator options for Auto-Protect scans of Internet email.

You can configure the following options:

- Whether or not to display a progress window on the client computer when an email message is sent.
- Whether or not to display an icon in the notification area to indicate the transmission status of the email.

Both options are enabled by default.

### To configure progress notifications

- 1 On the Antivirus and Antispyware Policy page, click **Internet Email Auto-Protect**.
- 2 On the Notifications tab, under Progress Notifications, do the following actions:
  - Check or uncheck **Display a progress indicator when email is being sent**.
  - Check or uncheck **Display a notification area icon**.
- 3 If you are finished with the configuration for this policy, click **OK**.

# Using administrator-defined scans

This chapter includes the following topics:

- [About using administrator-defined scans](#)
- [Adding scheduled scans to an Antivirus and Antispyware Policy](#)
- [Configuring on-demand scan options](#)
- [Running on-demand scans](#)
- [Configuring scan progress options for administrator-defined scans](#)
- [Setting advanced options for administrator-defined scans](#)

## About using administrator-defined scans

Administrator-defined scans include antivirus and antispyware scheduled scans and on-demand scans. You configure options for these types of scans as part of an Antivirus and Antispyware Policy.

You use scheduled scans and on-demand scans to supplement the protection that Auto-Protect provides. Auto-Protect provides protection when you read and write files. Scheduled scans and on-demand scans can scan any files that exist on your client computers. They can also protect memory, load points, and other important locations on your client computers.

---

**Note:** For managed clients, Symantec Endpoint Protection provides a default scheduled scan that scans all files, folders, and locations on the client computers.

---

Some options for administrator-defined scans are similar to the options for Auto-Protect scans. The similar options include the detection actions and the notifications that you specify.

See [“Configuring the options that apply to antivirus and antispyware scans”](#) on page 381.

## Adding scheduled scans to an Antivirus and Antispyware Policy

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

You can save your scheduled scan settings as a template. You can use any scan that you save as a template as the basis for a different Antivirus and Antispyware Policy. The scan templates can save you time when you configure multiple Antivirus and Antispyware Policies. A scheduled scan template is included by default in the policy. The default scheduled scan scans all files and directories.

You can click Help for more information about the options that are used in this procedure.

### To add a scheduled scan to an Antivirus and Antispyware Policy

- 1 On the Antivirus and Antispyware Policy page, click **Administrator-defined Scans**.
- 2 On the Scans tab, under Scheduled Scans, click **Add**.
- 3 In the Add Scheduled Scan dialog box, click **Create a new scheduled scan**.
- 4 Click **OK**.
- 5 In the Add Scheduled Scan dialog box, on the Scan Details tab, type a name and description for this scheduled scan.
- 6 Select the type of scan (Active, Full, or Custom).
- 7 If you selected Custom, under Scanning, you can specify which directories to scan.
- 8 Under File types, click **Scan all files** or **Scan only selected extensions**.  
See [“Configuring scans of selected file extensions”](#) on page 381.
- 9 Under Enhance the scan by checking, check or uncheck **Memory**, **Common infection locations**, or **Well-known virus and security risk locations**.

- 10 Click **Advanced Scanning Options**.
- 11 Set any of the options for compressed files, storage migration, or performance optimization.
- 12 Click **OK** to save the advanced scanning options for this scan.
- 13 On the Schedule tab, under Scanning schedule, set the frequency and the time at which the scan should run.
- 14 On the Actions tab, set any of the options.  
See [“Configuring actions for known virus and security risk detections”](#) on page 384.
- 15 On the Notifications tab, set any of the options.  
See [“About notification messages on infected computers”](#) on page 385.
- 16 If you want to save this scan as a template, check **Save a copy as a Scheduled Scan Template**.
- 17 Click **OK**.

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

- 1 On the Antivirus and Antispyware Policy page, click **Administrator-defined Scans**.
- 2 On the Scans tab, under Scheduled scans, click **Add**.
- 3 In the Add Scheduled Scan dialog box, click **Create a scheduled scan from a Scheduled Scan Template**.
- 4 Select the scan template that you want to use for this policy.
- 5 Click **OK**.

## Setting options for missed scheduled scans

If a computer misses a scheduled scan for some reason, the Symantec Endpoint Protection client tries to perform the scan for a specific time interval. If the client cannot start the scan within the time interval, it does not run the scan.

If the user who defined a scan is not logged in, the client software runs the scan anyway. You can specify that the client does not run the scan if the user is logged off.

[Table 31-1](#) describes the default time intervals.

**Table 31-1** Default time intervals

Scan frequency	Default interval
Daily scans	8 hours
Weekly scans	3 days
Monthly scans	11 days

If you do not want to use the default setting, you can specify a different time interval in which to try a scheduled scan.

You can click Help for more information about the options that are used in this procedure.

You can set options for missed scheduled scans when you create a scheduled scan or when you edit an existing scheduled scan.

**To set options for missed scheduled scans**

- 1 On the Antivirus and Antispyware Policy page, click **Administrator-defined Scans**.
- 2 On the Scans tab, under Scheduled Scans, do one of the following actions:
  - Click **Add**, and then in the Add Scheduled Scan dialog box, make sure Create a new scheduled scan is checked. Click **OK**.
  - Select a scan in the list, and then click **Edit**.
- 3 On the Schedule tab, under Missed Scheduled Scans, check **Specify the time to wait before retrying**.

Type the number or use the arrows to specify the time interval for the client to retry the scheduled scan.
- 4 Click **OK**.

## Editing, deleting, or disabling scheduled scans

You can edit, delete, or disable scheduled scans in an Antivirus and Antispyware Policy. The changes take effect the next time that you apply the policy.

You can click Help for more information about the options that are used in this procedure.

**To edit a scheduled scan**

- 1 On the Antivirus and Antispyware Policy page, click **Administrator-defined Scans**.
- 2 On the Scans tab, select the scan that you want to edit, and then click **Edit**.

- 3 In the Edit Scheduled Scan dialog box, make any of the edits that you want.
- 4 Click **OK**.

#### To delete a scheduled scan

- 1 On the Antivirus and Antispyware Policy page, click **Administrator-defined Scans**.
- 2 On the Scans tab, select the scan that you want to delete.
- 3 Click **Delete**.
- 4 In the message that appears, click **Yes**.

#### To disable a scheduled scan

- 1 On the Antivirus and Antispyware Policy page, click **Administrator-defined Scans**.
- 2 On the Scans tab, select the scan that you want to disable in this policy.
- 3 Click **Edit**.
- 4 In the Edit Scheduled Scan dialog box, on the Schedule tab, uncheck **Enable scan**.
- 5 Click **OK**.

## Configuring on-demand scan options

You can configure options for the custom scans that you want to run on demand. You run the on-demand scans manually from the Clients page. You can also run the on-demand scans from the Monitors page in the management console.

You cannot configure a scan name or a description for the scan options. The client uses the options whenever you run a custom on-demand scan from the management console on the client computer.

---

**Note:** You can run an Active Scan or a full scan on demand.

---

See [“About administrator-defined scans”](#) on page 367.

The settings for on-demand scans are similar to the settings for scheduled scans.

See [“Adding scheduled scans to an Antivirus and Antispyware Policy”](#) on page 412.

You can click Help for more information about the options that are used in this procedure.

### To configure settings for on-demand scans

- 1 On the Antivirus and Antispyware Policy page, click **Administrator-defined Scans**.
- 2 On the Scans tab, under Administrator On-demand Scan, click **Edit**.
- 3 In the Edit Administrator On-demand Scan dialog box, on the Scan Details tab, under Scanning, click **Edit Folders**.  
By default, the scan includes all folders.
- 4 In the Edit Folders dialog box, select the desired folders, and then click **OK**.
- 5 In the Edit Administrator On-demand Scan dialog box, under File types, click **Scan all files** or **Scan only selected extensions**.  
See [“About scanning selected extensions or folders”](#) on page 370.
- 6 Under Enhance the scan by checking, check or uncheck **Memory**, **Common infection locations**, or **Well-known virus and security risk locations**.
- 7 Click **Advanced Scanning Options**.
- 8 Set any of the options for compressed files, storage migration, or performance optimization.
- 9 Click **OK** to save the advanced options for this scan.
- 10 On the Actions tab, set any of the options.  
See [“Configuring actions for known virus and security risk detections”](#) on page 384.
- 11 On the Notifications tab, set any of the options.  
See [“About notification messages on infected computers”](#) on page 385.
- 12 Click **OK**.

## Running on-demand scans

You can run a scan remotely from the management console. You can run the scan from the Clients tab in the console. You can also run the scan from computer status logs that you generate on the Monitors tab.

See [“Running commands and actions from logs”](#) on page 186.

You can run an active, full, or custom on-demand scan. The custom scan uses the settings that are configured for on-demand scans in the Antivirus and Antispyware Policy.

By default, the scan scans the following types of items:



- All directories
- All file types
- Memory
- Common infection locations
- Well-known virus and security risk locations

See [“Configuring on-demand scan options”](#) on page 415.

You can click Help for more information about the options that are used in the procedures.

---

**Note:** If you issue a restart command on a client computer that runs an on-demand scan, the scan stops and the client computer restarts. The scan does not restart.

---

#### To run an on-demand scan on a group

- 1 In the console, click **Clients**.
- 2 Under View Clients, right-click the group that includes the computers that you want to scan.
- 3 Click **Run Command on Group > Scan**.
- 4 In the Select Scan Type dialog box, select Active Scan, Full Scan, or Custom Scan.
- 5 Click **OK**.
- 6 In the message that appears, click **Yes**.
- 7 In the confirmation message that appears, click **OK**.

#### To run an on-demand scan on a computer or user

- 1 In the console, click **Clients**.
- 2 In the right pane, under Clients, select the computers and users for which you want to run a scan.
- 3 Right-click the selection, and then click **Run Command on Clients > Scan**.
- 4 In the message that appears, click **Yes**.
- 5 In the Select Scan Type dialog box, select Active Scan, Full Scan, or Custom Scan.
- 6 Click **OK**.
- 7 In the confirmation message that appears, click **OK**.

## Configuring scan progress options for administrator-defined scans

You can configure whether or not the Scan Results dialog box appears on client computers. If you allow the dialog box to appear on client computers, users are always allowed to pause or delay an administrator-defined scan.

You can allow users to stop a scan entirely. You can also configure options for how users pause or delay scans.

The possible user actions are defined as follows:

Paused scan	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.
Snoozed scan	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.
Stopped scan	When a user stops a scan, the scan usually stops immediately. If a user stops a scan while the client software scans a compressed file, the scan does not stop immediately. In this case, the scan stops as soon as the compressed file has been scanned. A stopped scan does not restart.

A paused scan automatically restarts after a specified time interval elapses.

You can click Help for more information about the options that are used in this procedure.

### To configure scan progress options for administrator-defined scans

- 1 On the Antivirus and Antispyware Policy page, click **Administrator-defined Scans**.
- 2 On the Advanced tab, under Scan Progress Options, click **Show scan progress** or **Show scan progress if risk detected**.
- 3 To automatically close the scan progress indicator after the scan completes, check **Close the scan progress window when done**.
- 4 Check **Allow user to stop scan**.
- 5 Click **Pause Options**.

- 6 In the Scan Pause Options dialog box, do any of the following actions:
  - To limit the time that a user may pause a scan, check **Limit the time the scan may be paused**, and then type a number of minutes. The range is 3 to 180.
  - To limit the number of times a user may delay (or snooze) a scan, in the Maximum number of snooze opportunities box, type a number between 1 and 8.
  - By default, a user can delay a scan for 1 hour. To change this limit to 3 hours, check **Allow users to snooze the scan for 3 hours**.
- 7 Click **OK**.

## Setting advanced options for administrator-defined scans

You can set advanced options for scheduled scans and on-demand scans.

You can click Help for more information about the options that are used in the procedure.

### To set advanced options for administrator-defined scans

- 1 On the Antivirus and Antispyware Policy page, click **Administrator-defined Scans**.
- 2 On the Advanced tab, under Scheduled Scans, check or uncheck the following options:
  - **Delay scheduled scans when running on batteries**
  - **Allow user-defined scheduled scans to run when scan author is not logged on**
- 3 Under Startup and Triggered Scans, check or uncheck the following options:
  - **Run startup scans when users log on**
  - **Allow users to modify startup scans**
  - **Run an Active Scan when new definitions arrive**
- 4 Click **OK**.



# Configuring Network Threat Protection

- [Basic Network Threat Protection settings](#)
- [Configuring intrusion prevention](#)
- [Customizing Network Threat Protection](#)



# Basic Network Threat Protection settings

This chapter includes the following topics:

- [About Network Threat Protection and network attacks](#)
- [About the firewall](#)
- [About working with Firewall Policies](#)
- [About firewall rules](#)
- [Adding blank rules](#)
- [Adding rules with the Add Firewall Rule Wizard](#)
- [Adding inherited rules from a parent group](#)
- [Importing and exporting rules](#)
- [Editing and deleting rules](#)
- [Copying and pasting rules](#)
- [Changing the order of rules](#)
- [Enabling and disabling rules](#)
- [Enabling Smart traffic filtering](#)
- [Enabling traffic and stealth settings](#)
- [Configuring peer-to-peer authentication](#)

## About Network Threat Protection and network attacks

Network attacks take advantage of the way that computers transfer information. The client can protect computers by monitoring the information that comes into and out of the computer, and by blocking attack attempts.

Information travels across the Internet in the form of packets. Each packet includes a header that contains information about the sending computer, the intended recipient, how the data in the packet should be processed, and the port that should receive the packet.

Ports are the channels that divide the stream of information that comes from the Internet into separate paths that individual applications handle. When Internet applications run on a computer, they listen to one or more ports and accept the information that is sent to these ports.

Network attacks take advantage of weaknesses in specific Internet programs. Attackers use the tools that send the packets that contain malicious programming code to a particular port. If an application that is vulnerable to this attack listens to that port, the code can let the attacker gain access to, disable, or even take control of the computer. The programming code that is used to generate the attacks may be contained inside of a single packet or span several packets.

You can install the client with default settings for Network Threat Protection. In most cases you do not have to change the settings. It is generally safe to leave the settings as they are. However, if you have a detailed understanding of networks, you can make many changes in the client firewall to fine-tune the client computer's protection.

## How Symantec Endpoint Protection protects computers against network attacks

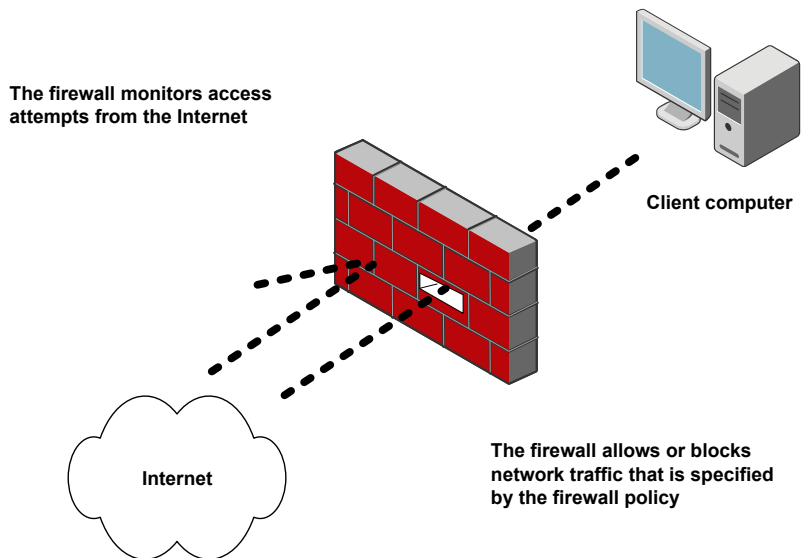
The Symantec Endpoint Protection client includes the following tools that protect computers in your organization from intrusion attempts:

Firewall	Monitors all Internet communication and creates a shield that blocks or limits the attempts to view information on the computer.
Intrusion prevention	Analyzes all inbound information and outbound information for the data patterns that are typical of an attack.  See <a href="#">“About the intrusion prevention system”</a> on page 447.



## About the firewall

The Symantec Endpoint Protection firewall is software that provides a barrier between the computer and the Internet. The firewall prevents unauthorized users from accessing the computers and the networks that connect to the Internet. It detects possible hacker attacks, protects personal information, and eliminates unwanted sources of network traffic.



All the information that enters or leaves the private network must pass through the firewall, which examines the information packets. The firewall blocks the packets that do not meet the specified security criteria. The way the firewall examines the information packets is through the use of a Firewall Policy. Firewall Policies consist of one or more rules that work together to allow or block users from accessing the network. Only authorized traffic can pass. The Firewall Policy defines the authorized traffic.

The firewall works in the background. You determine the level of interaction that you want users to have with the client by permitting or blocking their ability to configure firewall rules and firewall settings. Users might interact with the client only when it notifies them of new network connections and possible problems, or they might have full access to the user interface.

See [“About firewall rules”](#) on page 427.

## About working with Firewall Policies

The Symantec Endpoint Protection Manager includes a default Firewall Policy with firewall rules and firewall settings for the office environment. The office environment is normally under the protection of corporate firewalls, boundary packet filters, or antivirus servers. Therefore, it is normally more secure than most home environments, where limited boundary protection is available.

When you install the console for the first time, it adds a default Firewall Policy to each group automatically. Every time you add a new location, the console copies a Firewall Policy to the default location automatically.

If the default protection is not appropriate, you can customize the Firewall Policy for each location, such as for a home site or customer site. If you do not want the default Firewall Policy, you can edit it or replace it with another shared policy.

Firewall Policies include the following elements:

Firewall rules	<p>Monitors all Internet communication and creates a shield that blocks or limits attempts to view information on the computer. Firewall rules can make the computer invisible to others on the Internet.</p> <p>Firewall rules protect remote users from hacker attacks and prevents hackers from gaining backdoor access to the corporate network through these computers. You can notify users when a firewall rule blocks an application on their computer.</p>
Smart traffic filters	<p>Allows the specific types of traffic that are required on most networks such as DHCP, DNS, and WINS traffic.</p> <p>See <a href="#">“Enabling Smart traffic filtering”</a> on page 443.</p>
Traffic and stealth settings	<p>Detects and blocks traffic that comes from certain drivers, protocols, and other sources.</p> <p>See <a href="#">“Enabling traffic and stealth settings”</a> on page 444.</p>
Peer-to-peer authentication settings	<p>Blocks a remote computer from connecting to a client computer until the client computer has authenticated that remote computer.</p> <p>See <a href="#">“Configuring peer-to-peer authentication”</a> on page 445.</p>

You can set a location to client control or mixed control so that the user can customize the Firewall Policy.

See [“Configuring Network Threat Protection settings for mixed control”](#) on page 463.

You create and edit Firewall Policies similarly to the way you create and modify other types of policies. You can assign, withdraw, replace, copy, export, import, or delete a Firewall Policy.

You typically assign a policy to multiple groups in your security network. You can create a non-shared, location-specific policy if you have specific requirements for a particular location.

You should be familiar with the basics of policy configuration to work with policies.

See [“About working with policies”](#) on page 322.

## About firewall rules

Firewall rules control how the client protects the client computer from malicious inbound traffic and malicious outbound traffic. The firewall automatically checks all the inbound and the outbound packets against these rules. The firewall then allows or blocks the packets that are based on the information that is specified in rules. When a computer tries to connect to another computer, the firewall compares the type of connection with its list of firewall rules.

### About the elements of a firewall rule

In general, a firewall rule describes the conditions in which a network connection may be allowed or denied. You use the following criteria to define a firewall rule:

Triggers	Applications, hosts, protocols, and network adapters
	When the firewall evaluates the rule, all the triggers must be true for a positive match to occur. If any one trigger is not true in relation to the current packet, the firewall cannot apply the rule. You can combine the trigger definitions to form more complex rules, such as to identify a particular protocol in relation to a specific destination address.
Conditions	Schedule and screen saver state
	The conditional parameters do not describe an aspect of a network connection. Instead, the conditional parameters determine the active state of a rule. You may define a schedule or identify a screen saver state that dictates when a rule is considered to be active or inactive. The conditional parameters are optional and if not defined, not significant. The firewall does not evaluate inactive rules.

Actions Allow or block, and log or do not log

The action parameters specify what actions the firewall takes when it successfully matches a rule. If the rule matches and is selected in response to a received packet, the firewall performs all actions. The firewall either allows or blocks the packet and logs or does not log the packet. If the firewall allows traffic, it lets the traffic that the rule specifies access the network. If the firewall blocks traffic, it blocks the traffic that the rule specifies so that it does not access the network.

A rule that combines all criteria might allow traffic to IP address 192.58.74.0 on remote port 80 between 9 AM and 5 PM daily.

## About application triggers

When the application is the only trigger you define in a rule that allows traffic, the firewall allows the application to perform any network operation. The application is the significant value, not the network operations that the application performs. For example, suppose you allow Internet Explorer and you define no other triggers. Users can access the remote sites that use HTTP, HTTPS, FTP, Gopher, and any other protocol that the Web browser supports. You can define additional triggers to describe the particular network protocols and hosts with which communication is allowed.

Application-based rules may be difficult to troubleshoot because an application may use multiple protocols. For example, if the firewall processes a rule that allows Internet Explorer before a rule that blocks FTP, the user can still communicate with FTP. The user can enter an FTP-based URL in the browser, such as `ftp://ftp.symantec.com`.

You should not use application rules to control traffic at the network level. For example, a rule that blocks or limits the use of Internet Explorer would have no effect should the user use a different Web browser. The traffic that the other Web browser generates would be compared against all other rules except the Internet Explorer rule. Application-based rules are more effective when the rules are configured to block the applications that send and receive traffic.

---

**Note:** If Trend Micro PC-cillin IS 2007 and the Symantec Endpoint Protection client are installed on the same computer, firewall rules for a specific Web browser do not work. Trend Micro PC-cillin delivers Web traffic to its own proxy software. In Trend Micro PC-cillin, you must disable the Web site access controls and data threat prevention option.

---

## About host triggers

When you define host triggers, you specify the host on both sides of the described network connection.

Traditionally, the way to express the relationship between hosts is referred to as being either the source or destination of a network connection.

You can define the host relationship in either one of the following ways:

**Source and destination** The source host and destination host is dependent on the direction of traffic. In one case the local client computer might be the source, whereas in another case the remote computer might be the source.

The source and the destination relationship is more commonly used in network-based firewalls.

**Local and remote** The local host is always the local client computer, and the remote host is always a remote computer that is positioned elsewhere on the network. This expression of the host relationship is independent of the direction of traffic.

The local and the remote relationship is more commonly used in host-based firewalls, and is a simpler way to look at traffic.

Figure 32-1 illustrates the source and destination relationship with respect to the direction of traffic.

**Figure 32-1** Source and destination hosts

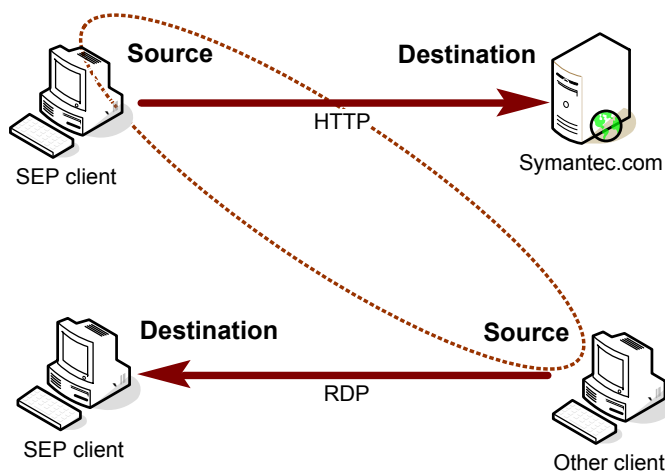
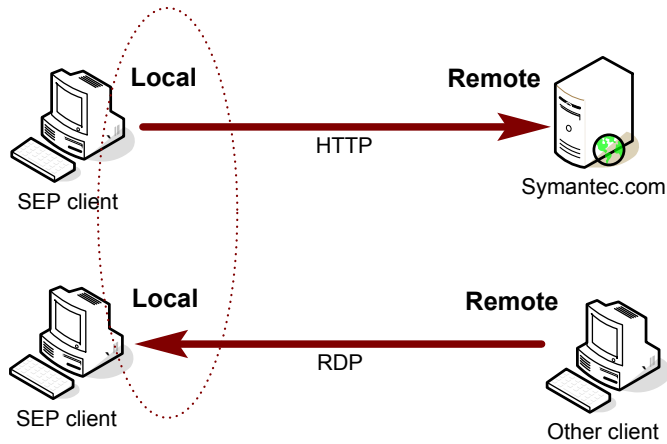


Figure 32-2 illustrates the local host and remote host relationship with respect to the direction of traffic.

Figure 32-2 Local and remote hosts



You can define multiple source hosts and multiple destination hosts. The hosts that you define on either side of the connection are evaluated by using an OR statement. The relationship between the selected hosts is evaluated by using an AND statement.

For example, consider a rule that defines a single local host and multiple remote hosts. As the firewall examines the packets, the local host must match the relevant IP address. However, the opposing sides of the address may be matched to any remote host. For example, you can define a rule to allow HTTP communication between the local host and either symantec.com, yahoo.com, or google.com. The single rule is the same as three rules.

See [“Adding hosts and host groups to a rule”](#) on page 465.

## About network service triggers

A network service trigger identifies one or more network protocols that are significant in relation to the described network traffic.

You can define the following types of protocols:

TCP	Port or port ranges
UDP	Port or port ranges
ICMP	Type and code

IP	Protocol number (IP type) Examples: Type 1 = ICMP, Type 6 = TCP, Type 17 = UDP
Ethernet	Ethernet frame type Examples: Type 0x0800 = IPv4, Type = 0x8BDD = IPv6, Type 0x8137 = IPX

When you define TCP-based or UDP-based service triggers, you identify the ports on both sides of the described network connection. Traditionally, ports are referred to as being either the source or the destination of a network connection.

You can define the network service relationship in either of the following ways:

Source and destination	The source port and destination port are dependent on the direction of traffic. In one case the local client computer might own the source port, whereas in another case the remote computer might own the source port.
Local and remote	The local host computer always owns the local port, and the remote computer always owns the remote port. This expression of the port relationship is independent of the direction of traffic.

You specify the direction of traffic when you define the protocol.

You can define multiple protocols. For example, a rule might include the ICMP, IP, and TCP protocols. The rule describes multiple types of connections that may occur between the identified client computers, or are used by an application.

## About network adapter triggers

When you define a network adapter trigger, the rule is relevant only to the traffic that is transmitted or received by using the specified type of adapter.

You can specify one of the following types of adapters:

- Ethernet
- Wireless
- Dial-up
- Any VPN
- Vender-specific virtual adapters

When you define a particular type of adapter, consider how that adapter is used. For example, if a rule allows outbound HTTP traffic from Ethernet adapters, then HTTP is allowed through all the installed adapters of the same type. The only exception is if you also specify local host addresses. The client computer may use

multi-NIC servers and the workstations that bridge two or more network segments. To control traffic relative to a particular adapter, the address scheme of each segment must be used rather than the adapter itself.

## About the rule processing order

Firewall rules are ordered sequentially, from highest to lowest priority, or from the top to bottom in the Rules list. The firewall inspects the rules in this order. If the first rule does not specify how to handle a packet, the firewall inspects the second rule for information on how to handle a packet. This process continues until the firewall finds a match. After the firewall finds a match, the firewall takes the action that the rule specifies, and subsequent lower priority rules are not inspected. For example, if a rule that blocks all traffic is listed first, followed by a rule that allows all traffic, the client blocks all traffic.

[Table 32-1](#) shows the order in which the firewall processes the rules and the settings.

**Table 32-1** Sequence for processing firewall rules, IPS signatures, and settings

Priority	Setting
First	Custom IPS signatures
Second	Intrusion prevention settings, traffic settings, and stealth settings
Third	Smart traffic filters
Fourth	Firewall rules
Fifth	Port scan checking
Sixth	IPS signatures that are downloaded through LiveUpdate

The Rules list contains a blue dividing line. The dividing line sets the priority of rules in the following situations:

- When a subgroup inherits rules from a parent group.
- When the client is set to mixed control. The firewall processes both server rules and client rules.

[Figure 32-3](#) displays the Rules list and the dividing blue line.



**Figure 32-3** Rules list

No	En...	Name	Severity	Application	Host	Time	Service	Adapter	Screen...	Action	Logging	Create...	Description
1	<input checked="" type="checkbox"/>	Rule 0	5-Major	Any	Any	Any	Any	All Ada...	Any	Allow	None	Shar...	
2	<input checked="" type="checkbox"/>	Allow wireless EAPOL	10-Minor	Any	Any	Any	Ethe...	All Ada...	Any	Allow	None	Shar...	
3	<input checked="" type="checkbox"/>	Allow Fragmented Pa...	10-Minor	Any	Any	Any	P-1f...	All Ada...	Any	Allow	None	Shar...	
4	<input checked="" type="checkbox"/>	Block Local File Shari...	10-Minor	Any	Any	Any	TCP...	All Ada...	Any	Block	Write1...	Shar...	
5	<input type="checkbox"/>	Allow VPN	5-Major	Any	Any	Any	UDP... VPN... VPN... VPN... VPN... VPN...	All Ada...	Any	Allow	None	Shar...	
6	<input checked="" type="checkbox"/>	Allow All Applications	10-Minor	*	Any	Any	Any	All Ada...	Any	Allow	None	Shar...	
7	<input checked="" type="checkbox"/>	Allow PING	10-Minor	Any	Any	Any	ICMP...	All Ada...	Any	Allow	None	Shar...	

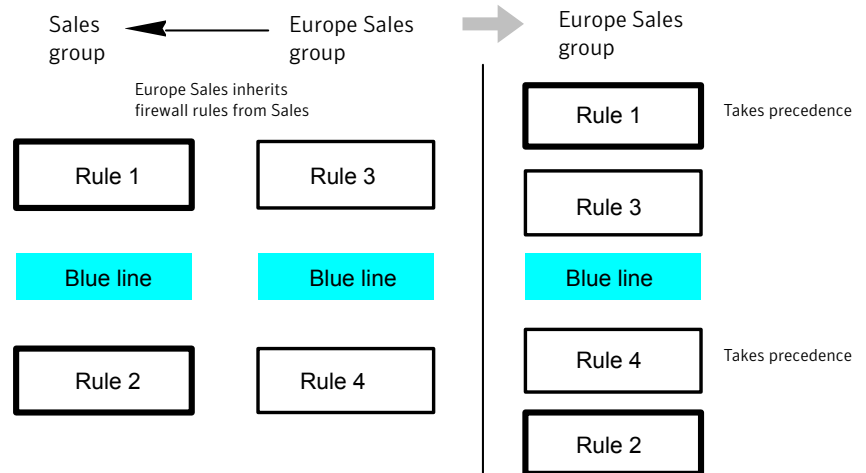
### About inherited rules

The firewall processes inherited firewall rules in the Rules list as follows:

- Above the blue dividing line, the rules that the policy inherits take precedence over the rules that you create.
- Under the blue dividing line, the rules that you create take precedence over the rules that the policy inherits.

Figure 32-4 displays how the Rules list orders rules when a subgroup inherits rules from a parent group. In this example, the Sales group is the parent group. The Europe Sales group inherits from the Sales group.

**Figure 32-4** Inherited firewall rules



See [“Adding inherited rules from a parent group”](#) on page 439.

## About server rules and client rules

Rules are categorized as either server rules or client rules. Server rules are the rules that you create in the Symantec Endpoint Protection Manager console and that are downloaded to the Symantec Endpoint Protection client. Client rules are the rules that the user creates on the client.

[Table 32-2](#) describes the relationship between the client's user control level and the user's interaction with the firewall rules.

**Table 32-2** User control level and rule status

User control level	User interaction
Server control	The client receives server rules but the user cannot view them. The user cannot create client rules.
Mixed control	The client receives server rules. The user can create client rules, which are merged with server rules and client security settings.
Client control	The client does not receive server rules. The user can create client rules. You cannot view client rules.

See [“Configuring user interface settings”](#) on page 108.

For clients in mixed control, the firewall processes server rules and client rules in a particular order.

[Table 32-3](#) lists the order that the firewall processes server rules and client rules and client settings.

**Table 32-3** Server rules and client rules processing priority

Priority	Rule type or setting
First	Server rules with high priority levels (rules above the blue line in the Rules list)
Second	Client rules
Third	Server rules with lower priority levels (rules under the blue line in the Rules list)  On the client, server rules under the blue line are processed after client rules.
Fourth	Client security settings
Fifth	Client application-specific settings

On the client, users can modify a client rule or security setting, but users cannot modify a server rule.

---

**Warning:** If the client is in mixed control, users can create a client rule that allows all traffic. This rule overrides all server rules under the blue line.

---

See [“Changing the order of rules”](#) on page 442.

## About stateful inspection

The firewall uses stateful inspection, a process that tracks information about current connections such as source and destination IP addresses, ports, and applications. The client makes traffic flow decisions by using this connection information before it inspects firewall rules.

For example, if a firewall rule permits a client to connect to a Web server, the firewall logs the connection information. When the server replies, the firewall discovers that a response from the Web server to the client is expected, and permits the Web server traffic to flow to the initiating client without inspecting the rulebase. A rule must permit the initial outbound traffic before the firewall logs the connection.

Stateful inspection lets you simplify rulebases because you do not have to create the rules that permit traffic in both directions for traffic that is typically initiated in one direction only. Client traffic that is typically initiated in one direction includes Telnet (port 23), HTTP (port 80), and HTTPS (port 443). Clients initiate this traffic outbound, so you only have to create a rule that permits outbound traffic for these protocols. The firewall permits the return traffic.

By configuring only outbound rules, you increase client security in the following ways:

- Reduce rulebase complexity.
- Eliminate the possibility that a worm or other malicious program can initiate connections to a client on the ports that are configured for outbound traffic only. You can also configure inbound rules only, for traffic to clients that clients do not initiate.

Stateful inspection supports all rules that direct TCP traffic. Stateful inspection does not support the rules that filter ICMP traffic. For ICMP traffic, you must create the rules that permit the traffic in both directions when necessary. For example, for clients to use the ping command and receive replies, you must create a rule that permits ICMP traffic in both directions.

Because the firewall is stateful in nature, you only need to create rules that initiate a connection, not the characteristics of a particular packet. All packets belonging

to an allowed connection are implicitly allowed as being an integral part of that same connection.

## About UDP connections

For UDP communications, the client analyzes the first UDP datagram and applies the action that is taken on the initial datagram to all subsequent UDP datagrams for the current program session. Inbound or outbound traffic between the same computers is considered part of the UDP connection.

For stateful UDP traffic, when a UDP connection is made, the inbound UDP communication is allowed, even if the firewall rule blocks it. For example, if a rule blocks inbound UDP communications for a specific application, but you choose to allow an outbound UDP datagram, all inbound UDP communications are allowed for the current application session. For stateless UDP, you must create a firewall rule to allow the inbound UDP communication response.

A UDP session times out after 40 seconds if the application closes the port.

## Adding blank rules

When you create a new Firewall Policy, the policy includes several default rules. The default rules give you basic protection for an office environment. If you need additional firewall rules, you can add them.

You add rules in the following ways:

- Add a blank rule to the list and then manually configure it.
- Run the Firewall Rule Wizard.

See [“Adding rules with the Add Firewall Rule Wizard”](#) on page 438.

To simplify rulebase management, you must specify both the inbound and the outbound traffic in the rule whenever possible. You do not need to create inbound rules for traffic such as HTTP. The Symantec Endpoint Protection client uses stateful inspection for TCP traffic and does not need a rule to filter the return traffic that the clients initiate.

See [“About stateful inspection”](#) on page 435.

### To add blank rules

- 1 In the console, open a Firewall Policy.  
See [“About editing policies”](#) on page 327.
- 2 On the Firewall Policy page, click **Rules**.
- 3 On the Rules tab, under the Rules list, click **Add Blank Rule**.

- 4 In the **Name** text box, type a name for the rule.
- 5 In the Severity field, click the drop-down list and select one of the following options:
  - Critical
  - Major
  - Minor
  - Information
- 6 Right-click the **Application** field, click **Edit**, and in the Application List dialog box, define an application.  
See [“Adding applications to a rule”](#) on page 472.
- 7 Click **OK**.
- 8 Right-click the **Host** field, click **Edit**, and in the Host list, define a host.  
See [“Adding hosts and host groups to a rule”](#) on page 465.
- 9 Click **OK**.
- 10 Right-click the **Time** field, click **Edit**, and then set up a schedule.  
See [“Adding schedules to a rule”](#) on page 474.
- 11 Click **OK**.
- 12 Right-click the **Service** field, and then click **Edit** to add or configure a custom network service.  
See [“Adding network services to a rule”](#) on page 468.
- 13 Click **OK**.
- 14 Right-click the **Adapter** field and select one or more of the following items:
  - All Adapters
  - Any VPN
  - Dial-up
  - Ethernet
  - Wireless
  - More Adapters  
You can add and select from a list of vendor-specific adaptersSee [“Adding network adapters”](#) on page 470.
- 15 Right-click the **Screen Saver** field and select which state you want the screen saver to be in:

- On
  - Off
  - Any
- 16** Right-click the **Action** field and select the action you want the firewall to take when the traffic matches rule:
- Allow
  - Block
  - Ask
- 17** Right-click the **Logging** field and select one or more logging actions you want the firewall to take when the traffic matches the rule:
- Write to Traffic Log
  - Write to Packet Log
  - Send Email Alert
- See [“Configuring email messages for traffic events”](#) on page 476.
- The Created At field is not editable. If the policy is shared, the field displays the term Shared. If the policy is not shared, the field displays the name of the group that the non-shared policy is assigned to.
- 18** Right-click the **Description** field, and then click **Edit**.
- 19** In the Enter Description dialog box, type an optional description for the rule, and then click **OK**.
- 20** When you are finished adding the rule, do one of the following actions:
- Add another rule.
  - Add Smart traffic filtering settings or traffic and stealth settings.  
See [“Enabling Smart traffic filtering”](#) on page 443.  
See [“Enabling traffic and stealth settings”](#) on page 444.
  - If you are done with the configuration of the policy, click **OK**.
- 21** If you are prompted, assign the policy to a location.  
See [“Assigning a shared policy”](#) on page 329.

## Adding rules with the Add Firewall Rule Wizard

Use the Add Firewall Rule Wizard to create one of the following types of rules:

Application rules	A rule that is based on a specific running process that attempts to use network resources
Host rules	A rule that is based on the endpoints of network connections
Service rules	A rule that is based on the protocols that are used by network connections

You may need to include two or more criteria to describe specific network traffic, such as a particular protocol that originates from a specific host. You must configure the rule after you add it, because the Add Firewall Rule Wizard does not configure new rules with multiple criteria.

When you become familiar with how rules are defined and processed, you may want to add blank rules and configure the various fields as needed. A blank rule allows all traffic.

See [“Adding blank rules”](#) on page 436.

#### To add rules with the Add Firewall Rule Wizard

- 1 In the console, open a Firewall Policy.  
See [“About editing policies”](#) on page 327.
- 2 On the Firewall Policy page, click **Rules**.
- 3 On the Rules tab, under the Rules list, click **Add Rule**.
- 4 In the Add Firewall Rule Wizard, click **Next**.
- 5 In the Select Rule Type panel, select one of the types of rules.
- 6 Click **Next**.
- 7 Enter data on each panel to create the type of rule you selected.
- 8 For applications and hosts, click **Add More** to add additional applications and services.
- 9 When you are done, click **Finish**.
- 10 In the Rules list, right-click any field to edit the rule.
- 11 When you are finished with the configuration of this policy, click **OK**.

## Adding inherited rules from a parent group

You can add rules by inheriting only the rules from a parent group. To inherit the rules from a parent group, the subgroup's policy must be a non-shared policy.

---

**Note:** If the group inherits all of its policies from a parent group, this option is unavailable.

---

Inherited rules are automatically enabled. The subgroup's policy can inherit only the firewall rules that are enabled in the parent group. When you have inherited the rules, you can disable them, but you cannot modify them. As the new rules are added to the parent group's policy, the new rules are automatically added to the inheriting policy.

When the inherited rules appear in the Rules list, they are shaded in purple. Above the blue line, the inherited rules are added above the rules that you created. Below the blue line, the inherited rules are added below the rules that you created.

A Firewall Policy also inherits default rules, so the subgroup's Firewall Policy may have two sets of default rules. You may want to delete one set of default rules.

If you want to remove the inherited rules, you uninherit them rather than delete them. You have to remove all the inherited rules rather than the selected rules.

#### To add inherited rules from a parent group

- 1 In the console, open a Firewall Policy.  
See [“About editing policies”](#) on page 327.
- 2 On the Firewall Policy page, click **Rules**.
- 3 On the Rules tab, above the Rules list, check **Inherit Firewall Rules from Parent Group**.  
To remove the inherited rules, uncheck **Inherit Firewall Rules from Parent Group**.
- 4 Click **OK**.  
See [“Groups, inheritance, locations, and policies”](#) on page 308.

## Importing and exporting rules

You can export and import firewall rules and settings from another Firewall Policy so that you do not have to re-create them. For example, you can import a partial rule set from one policy into another. To import rules, you first have to export the rules to a .dat file and have access to the file.

The rules are added in the same order that they are listed in the parent policy with respect to the blue line. You can then change their processing order.



### To export rules

- 1 In the console, open a Firewall Policy.  
See [“About editing policies”](#) on page 327.
- 2 On the Firewall Policy page, click **Rules**.
- 3 In the Rules list, select the rules you want to export, right-click, and then click **Export**.
- 4 In the Export Policy dialog box, locate a directory to save the .dat file, type a file name, and then click **Export**.

### To import rules

- 1 In the console, open a Firewall Policy.  
See [“About editing policies”](#) on page 327.
- 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**.

## Editing and deleting rules

You can change firewall rules if they do not function the way that you want. To modify a rule is the same as to add a blank rule and then edit it.

You can delete any firewall rule, even a default rule. You cannot delete a rule in a policy that is inherited from a parent policy.

### To edit rules

- 1 In the console, open a Firewall Policy.  
See [“About editing policies”](#) on page 327.
- 2 In the Firewall Policy page, click **Rules**.
- 3 On the Rules tab, under the Rules list, double-click any column in a rule to edit the rule.
- 4 Edit any column in the rule table.  
See [“Adding blank rules”](#) on page 436.
- 5 Click **OK** to save your changes.

#### To delete rules

- 1 In the console, open a Firewall Policy.  
See [“About editing policies”](#) on page 327.
- 2 On the Firewall Policy page, click **Rules**.
- 3 On the Rules tab, select the rule you want to delete and below the Rules list, click **Delete**.
- 4 Click **Yes** to confirm that you want to delete the rule.
- 5 Click **OK**.

## Copying and pasting rules

You can copy and paste rules from the same policy or another policy.

#### To copy and paste rules

- 1 In the console, open a Firewall Policy.  
See [“About editing policies”](#) on page 327.
- 2 In the Firewall Policy page, click **Rules**.
- 3 On the Rules tab, right-click the rule you want to copy, and then click **Copy Rule**.
- 4 Right-click the row where you want the rule to be pasted, and then click **Paste Rule**.
- 5 Click **OK**.

## Changing the order of rules

The firewall processes the list of firewall rules from the top down. You can determine how the firewall processes firewall rules by changing their order. When you change the order, it affects the order for the currently selected location only.

#### To change the order of rules

- 1 In the console, open a Firewall Policy.  
See [“About editing policies”](#) on page 327.
- 2 In the Firewall Policy page, click **Rules**, and then select the rule that you want to move.
- 3 Do one of the following tasks:
  - To process this rule before the previous rule, click **Move Up**.

- To process this rule after the rule below it, click **Move Down**.
- 4 Click **OK**.

## Enabling and disabling rules

Rules must be enabled for the firewall to process them. You can disable a firewall rule if you need to allow specific access to a computer or application. The rule is disabled for the all locations if it is a shared policy, and only one location if it is a location-specific policy. The rule is also disabled for all inherited policies.

### To enable and disable rules

- 1 In the console, open a Firewall Policy.  
See [“About editing policies”](#) on page 327.
- 2 In the Firewall Policy page, click **Rules**.
- 3 On the Rules tab, select the rule you want to enable or disable, and then check or uncheck the check box in the Enabled column.
- 4 Click **OK**.

## Enabling Smart traffic filtering

Smart traffic filters allow communication between certain network services so that you do not have to define the rules that explicitly allow those services. You can enable Smart traffic filters to allow DHCP, DNS, and WINS traffic on most networks. The Smart traffic filters allow outbound requests and inbound replies for the network connections that have been configured to use DHCP, DNS, and WINS.

The filters allow DHCP, DNS, or WINS clients to receive an IP address from a server while protecting the clients against attacks from the network.

- If the client sends a request to the server, the client waits for five seconds to allow an inbound response.
- If the client does not send a request to the server, each filter does not allow the packet.

Smart filters allow the packet if a request was made. They do not block packets. The firewall rules allow or block packets.

---

**Note:** To configure these settings in mixed control, you must also enable these settings in the Client User Interface Mixed Control Settings dialog box.

---

See [“About mixed control”](#) on page 107.

#### To enable Smart traffic filtering

- 1 In the console, open a Firewall Policy.  
See [“About editing policies”](#) on page 327.
- 2 In the Firewall Policy page, click **Smart Traffic Filters**.
- 3 If not checked already, check any of the following check boxes:
  - **Enable Smart DHCP**
  - **Enable Smart DNS**
  - **Enable Smart WINS**For more information on these options, click **Help**.
- 4 Click **OK**.
- 5 If you are prompted, assign the policy to a location.  
See [“Assigning a shared policy”](#) on page 329.

## Enabling traffic and stealth settings

You can enable traffic settings to detect and block the traffic that communicates through drivers, NetBIOS, and token rings. You can also configure settings to detect the traffic that uses more invisible attacks.

---

**Note:** To configure these settings in mixed control, you must also enable these settings in the Client User Interface Mixed Control Settings dialog box.

---

See [“About mixed control”](#) on page 107.

#### To enable traffic and stealth settings

- 1 In the console, open a Firewall Policy.  
See [“About editing policies”](#) on page 327.
- 2 In the Firewall Policy page, click **Traffic and Stealth settings**.
- 3 If a check box is not checked already, check any one of the following check boxes:
  - **Enable NetBIOS protection**
  - **Allow token ring traffic**
  - **Enable reverse DNS lookup**

- **Enable anti-MAC spoofing**
- **Enable stealth mode Web browsing**
- **Enable TCP resequencing**
- **Enable OS fingerprint masquerading**

For more information on these options, click **Help**.

- 4 Click **OK**.
- 5 If you are prompted, assign the policy to a location.  
See [“Assigning a shared policy”](#) on page 329.

## Configuring peer-to-peer authentication

You can use peer-to-peer authentication to allow a remote client computer (peer) to connect to another client computer (authenticator) within the same corporate network. The authenticator temporarily blocks inbound TCP and UDP traffic from the remote computer until the remote computer passes the Host Integrity check.

The Host Integrity check verifies the following characteristics of the remote computer:

- The remote computer has both Symantec Endpoint Protection and Symantec Network Access Control installed.
- The remote computer meets the Host Integrity Policy requirements.

If the remote computer passes the Host Integrity check, the authenticator allows the remote computer to connect to it.

If the remote computer fails the Host Integrity check, the authenticator continues to block the remote computer. You can specify how long the remote computer is blocked before it can try to connect to the authenticator again. You can also specify certain remote computers to always be allowed, even if they would not pass the Host Integrity check. If you do not enable a Host Integrity Policy for the remote computer, the remote computer passes the Host Integrity check.

Peer-to-peer authentication information is displayed in the Compliance Enforcer Client log and in the Network Threat Protection Traffic log.

---

**Note:** Peer-to-peer authentication works in server control and mixed control, but not in client control.

---

---

**Warning:** Do not enable peer-to-peer authentication for the clients that are installed on the same computer as the management server. Otherwise, the management server cannot download policies to the remote computer if the remote computer fails the Host Integrity check.

---

**To configure peer-to-peer authentication**

- 1 In the console, open a Firewall Policy.  
See [“About editing policies”](#) on page 327.
- 2 In the Firewall Policy page, click **Peer-to-Peer Authentication Settings**.
- 3 On the Peer-to-Peer Authentication Settings pane, check **Enable peer-to-peer authentication**.
- 4 Configure each of the values that is listed on the page.  
For more information about these options, click **Help**.
- 5 To allow remote computers to connect to the client computer without being authenticated, check **Exclude hosts from authentication**, and then click **Excluded Hosts**.  
The client computer allows traffic to the computers listed in the Host List.
- 6 In the Excluded Hosts dialog box, click **Add** to add the remote computers that do not have to be authenticated.
- 7 In the Host dialog box, define the host by IP address, IP range, or the subnet, and then click **OK**.
- 8 In the Excluded Hosts dialog box, click **OK**.
- 9 When you are done with the configuration of this policy, click **OK**.
- 10 If you are prompted, assign the policy to a location.  
See [“Assigning a shared policy”](#) on page 329.

# Configuring intrusion prevention

This chapter includes the following topics:

- [About the intrusion prevention system](#)
- [Configuring intrusion prevention](#)
- [Creating custom IPS signatures](#)

## About the intrusion prevention system

The intrusion prevention system (IPS) is the Symantec Endpoint Protection client's second layer of defense after the firewall. The IPS is a network-based system that operates on every computer on which the client is installed and the intrusion prevention system is enabled. If a known attack is detected, one or more intrusion prevention technologies can automatically block it.

The intrusion prevention system scans each packet that enters and exits computers in the network for attack signatures. Attack signatures are the packet sequences that identify an attacker's attempt to exploit a known operating system or program vulnerability.

If the information matches a known attack, the IPS automatically discards the packet. The IPS can also sever the connection with the computer that sent the data for a specified amount of time. This feature is called active response, and it protects computers on your network from being affected in any way.

The client includes the following types of IPS engines that identify attack signatures.

Symantec IPS signatures	The Symantec IPS signatures use a stream-based engine that scans multiple packets. Symantec IPS signatures intercept network data at the session layer and capture segments of the messages that are passed back and forth between an application and the network stack.
Custom IPS signatures	The custom IPS signatures use a packet-based engine that scans each packet individually.

The intrusion prevention system logs the detected attacks in the Security log. You can enable the custom IPS signatures to log detected attacks in the Packet log.

## About the Symantec IPS signatures

The Symantec IPS examines packets in two ways. It scans each packet individually by looking for the patterns that do not adhere to specifications and that can crash the TCP/IP stack. It also monitors the packets as a stream of information. It monitors by looking for the commands that are directed at a particular service to exploit or crash the system. The IPS can remember the list of patterns or partial patterns from previous packets and can apply this information to subsequent packet inspections.

The IPS relies on an extensive list of attack signatures to detect and block suspicious network activity. The Symantec Security Response team supplies the known threat list, which you can update on the client by using Symantec LiveUpdate. You download the signatures to the console and then use a LiveUpdate Content Policy to download them to the client. The Symantec IPS engine and the corresponding set of IPS signatures are installed on the client by default.

See [“Configuring a LiveUpdate Content Policy”](#) on page 93.

You can also change the behavior of the Symantec IPS signatures.

See [“Changing the behavior of Symantec IPS signatures”](#) on page 451.

## About custom IPS signatures

The client contains an additional IPS engine that supports packet-based signatures. Both the stream-based and packet-based engines detect signatures in the network data that attack the TCP/IP stack, operating system components, and the application layer. But packet-based signatures can detect attacks in the TCP/IP stack earlier than stream-based signatures.



The packet-based engine does not detect the signatures that span multiple packets. The packet-based IPS engine is more limited in that it does not buffer partial matches and scans single packet payloads only.

Packet-based signatures examine a single packet that matches a rule. The rule specifies a protocol, port, source or destination IP address, or application. Certain attacks are commonly launched against specific applications. The custom signatures use application-based rules, which change dynamically for each packet. The rule is based on various criteria, such as application, TCP flag number, port, and protocol. For example, a custom signature can monitor the packets of information that are received for the string “phf” in GET / cgi-bin/phf? as an indicator of a CGI program attack. Each packet is evaluated for that specific pattern. If the packet of traffic matches the rule, the client allows or blocks the packet and optionally logs the event in the Packet log.

Signatures can cause false positives because they are often based on regular expressions and string matches. The custom signatures use both criteria to look for strings when trying to match a packet.

The client does not include custom signatures by default. You create custom IPS signatures.

See “[Creating custom IPS signatures](#)” on page 454.

## Configuring intrusion prevention

The default IPS settings protect the client computers against a wide variety of threats. You can customize the default settings for your network. You can customize the IPS settings in one or more of the following ways:

- Enable intrusion prevention settings.
- Change the behavior of specific attack signatures.
- Exclude specific computers from being scanned.
- Block an attacking computer automatically.
- Enable intrusion prevention notifications.

See “[Configuring notifications for Network Threat Protection](#)” on page 475.

- Create custom IPS signatures.

See “[Creating custom IPS signatures](#)” on page 454.

## About working with Intrusion Prevention Policies

Except for custom IPS signatures and intrusion prevention notifications, when you configure intrusion prevention, you create an Intrusion Prevention Policy. For custom IPS signatures, you create a custom IPS library.

You create and edit Intrusion Prevention Policies similar to the way you create and modify other types of policies. You can assign, withdraw, replace, copy, export, import, or delete an Intrusion Prevention Policy or Custom Intrusion Prevention Library.

You typically assign a policy to multiple groups in your security network. You can create a non-shared, location-specific policy if you have specific requirements for a particular location.

The procedures in this chapter assume that you are familiar with the basics of policy configuration.

See [“About working with policies”](#) on page 322.

## Enabling intrusion prevention settings

You can block certain types of attacks on the client, depending on the intrusion prevention technology that you select.

You must enable the intrusion prevention settings to enable either the Symantec IPS signature engine or the custom IPS signature engine. If you do not enable this setting, the client ignores possible attack signatures.

---

**Note:** To configure these settings in mixed control, you must also enable these settings in the Client User Interface Mixed Control Settings dialog box.

---

See [“Configuring Network Threat Protection settings for mixed control”](#) on page 463.

For more information about these options, click Help.

### To enable intrusion prevention settings

- 1 In the console, open an Intrusion Prevention Policy.  
See [“About editing policies”](#) on page 327.
- 2 On the Intrusion Prevention Policy page, click **Settings**.
- 3 On the Settings page, check the following check boxes that apply:
  - **Enable Intrusion Prevention**
  - **Enable denial of service detection**

- **Enable port scan detection**

4 When you finish configuring this policy, click **OK**.

See “[Setting up a list of excluded computers](#)” on page 453.

## Changing the behavior of Symantec IPS signatures

You may want to change the default behavior of the Symantec IPS signatures for the following reasons:

- To reduce the possibility of a false positive. In some cases, benign network activity may appear similar to an attack signature. If you receive repeated warnings about possible attacks, and you know that these attacks are being triggered by safe behavior, you can exclude the attack signature that matches the benign activity.
- To reduce resource consumption by reducing the number of attack signatures for which the client checks. However, you must be certain that an attack signature poses no threat before excluding it from blocking.

You can change the action that the client takes when the IPS recognizes an attack signature. You can also change whether the client logs the event in the Security log.

---

**Note:** To change the behavior of a custom IPS signature that you create or import, you edit the signature directly.

---

### To change the behavior of Symantec IPS signatures

- 1 In the console, open an Intrusion Prevention Policy.  
See “[About editing policies](#)” on page 327.
- 2 On the Intrusion Prevention Policy page, click **Exceptions**.
- 3 On the Exceptions page, click **Add**.
- 4 In the Add Intrusion Prevention Exceptions dialog box, do one of the following actions to filter the signatures:
  - To display the signatures in a particular category, select an option from the Show category drop-down list.
  - To display the signatures that are classified with a particular severity, select an option from the Show severity drop-down list.
- 5 Select one or more IPS signatures.  
To make the behavior for all signatures the same, click **Select All**.

- 6 Click **Next**.
  - 7 In the Signature Action dialog box, change the action from Block to Allow or from Allow to Block.
  - 8 Optionally, change the log action in either one of the following ways:
    - Change **Log the traffic** to **Do not log the traffic**.
    - Change **Do not log the traffic** to **Log the traffic**.
  - 9 Click **OK**.
- 10 Click **OK**.
  - 11 If you want to change the behavior of other signatures, repeat steps 3 to 10.
  - 12 When you finish configuring this policy, click **OK**.

See “[Viewing and changing the LiveUpdate Content Policy that is applied to a group](#)” on page 95.

#### To remove the exception

- 1 In the console, open an Intrusion Prevention Policy.  
See “[About editing policies](#)” on page 327.
- 2 On the Intrusion Prevention Policy page, click **Exceptions**.
- 3 On the Exceptions pane, select the exception you want to remove and click **Delete**.
- 4 When you are asked to confirm the deletion, click **Yes**.

## Blocking an attacking computer

If the Symantec Endpoint Protection client detects a network attack, it can automatically block the connection to ensure that the client computer is safe. The client activates an active response, which automatically blocks all communication to and from the attacking computer for a set period of time. The IP address of the attacking computer is blocked for a single location.

The attacker’s IP address is recorded in the Security log. In client control, users can unblock an attack by stopping the active response in the Security log.

If you set the client to mixed control, you can specify whether the setting is available or not available on the client for the user to enable. If not available, you must enable it in the Client User Interface Mixed Control Settings dialog box.

See “[Configuring Network Threat Protection settings for mixed control](#)” on page 463.

Updated IPS signatures, updated denial-of-service signatures, port scans, and MAC spoofing also trigger an active response.

#### To block an attacking computer

- 1 In the console, open an Intrusion Prevention Policy.  
See [“About editing policies”](#) on page 327.
- 2 On the Intrusion Prevention Policy page, click **Settings**.
- 3 On the Settings page, check **Automatically block an attacker's IP address**.
- 4 In the **Number of seconds during which to block IP address ... seconds** text box, specify the number of seconds to block potential attackers.  
Enter a number from one second to 999,999 seconds.
- 5 When you finish configuring this policy, click **OK**.

## Setting up a list of excluded computers

The Symantec Endpoint Protection client may define some normal Internet activities as attacks. For example, some Internet service providers scan the ports of the computer to ensure that you are within their service agreements. Or, you may have some computers in your internal network that you want to set up for testing purposes.

You can set up a list of computers for which the client does not match attack signatures or check for port scans or denial-of-service attacks. The client allows all inbound traffic and outbound traffic from these hosts, regardless of the firewall rules and settings or IPS signatures.

---

**Note:** You can also set up a list of computers that allows all inbound traffic and outbound traffic unless an IPS signature detects an attack. In this case, you create a firewall rule that allows all hosts.

---

#### To set up a list of excluded computers

- 1 In the console, open an Intrusion Prevention Policy.  
See [“About editing policies”](#) on page 327.
- 2 On the Intrusion Prevention Policy page, click **Settings**.
- 3 If not checked already, check **Enable excluded hosts** and then click **Excluded Hosts**.
- 4 In the Excluded Hosts dialog box, click **Add**.

- 5 In the Host dialog box, in the drop-down list, select one of the following host types:
  - DNS domain
  - DNS host
  - IP address
  - IP range
  - MAC address
  - Subnet
- 6 Enter the appropriate information that is associated with the host type you selected.

For more information about these options, click **Help**.
- 7 Click **OK**.
- 8 Repeat 4 and 7 to add additional devices and computers to the list of excluded computers.
- 9 To edit or delete any of the excluded hosts, select a row, and then click **Edit** or **Delete**.
- 10 Click **OK**.
- 11 When you finish configuring the policy, click **OK**.

## Creating custom IPS signatures

You can write your own signatures to identify a specific intrusion and reduce the possibility of signatures that cause a false positive. The more information you can add to a custom signature, the more effective the signature is.

When you create a custom library, you can organize signatures into signature groups to manage them more easily. You must add at least one signature group to a custom signature library before you add the signatures to the signature group. You can copy and paste signatures between groups and between libraries.

---

**Warning:** You must be familiar with the TCP, UDP, or ICMP protocols before you develop intrusion prevention signatures. An incorrectly formed signature can corrupt the custom IPS library and damage the integrity of the clients.

---

To create custom IPS signatures, you must complete the following steps:

- Create a custom IPS library.

- Add a signature.

#### To create a custom IPS library

- 1 In the console, click **Policies**, and then click **Intrusion Prevention**.
- 2 Under Tasks, click **Add Custom Intrusion Prevention Signatures**.
- 3 In the Custom Intrusion Prevention Signatures dialog box, type a name and optional description for the library.

The NetBIOS Group is a sample signature group with one sample signature. You can edit the existing group or add a new group.

- 4 To add a new group, on the Signatures tab, under the Signature Groups list, click **Add**.
- 5 In the Intrusion Prevention Signature Group dialog box, type a group name and optional description, and then click **OK**.

The group is enabled by default. If the signature group is enabled, all signatures within the group are enabled automatically. To retain the group for reference but to disable it, uncheck **Enable this group**.

- 6 Add a custom signature.

#### To add a custom signature

- 1 Add a custom IPS library.
- 2 On the Signatures tab, under Signatures for this Group, click **Add**.
- 3 In the Add Signature dialog box, type a name and optional description for the signature.
- 4 In the Severity drop-down list, select a severity level.

Events that match the signature conditions are logged with this severity.

- 5 In the Direction drop-down list, specify the traffic direction that you want the signature to check.
- 6 In the Content field, type the syntax of the signature.

For more information on the syntax, click **Help**.

- 7 If you want an application to trigger the signature, click **Add**.
- 8 In the Add Application dialog box, type the file name and an optional description for the application.

For example, to add the application Microsoft Internet Explorer, type the file name as **iexplore** or **iexplore.exe**. If you do not specify a file name, any application can trigger the signature.

**9** Click **OK**.

The added application is enabled by default. If you want to disable the application until a later time, uncheck the check box in the Enabled column.

**10** In the Action group box, select the action you want the client to take when the signature detects the event:

Block	Identifies and blocks the event or attack and records it in the Security Log
Allow	Identifies and allows the event or attack and records it in the Security Log
Write to Packet Log	Records the event or attack in the Packet Log

**11** 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.

**12** To add additional signatures to the signature group, repeat steps 2 to 11.

To edit or delete a signature, select it and then click **Edit** or **Delete**.

**13** If you are finished with the configuration of this library, click **OK**.

**14** If you are prompted to assign the custom IPS signatures to a group, click **Yes**.

**15** In the Assign Intrusion Prevention Policy dialog box, select the groups to which you want to assign the policy.

**16** Click **Assign**, and then click **Yes**.

## Assigning multiple custom IPS libraries to a group

After you create a custom IPS library, you assign it to a group rather than an individual location. You can later assign additional custom IPS libraries to the group.

### To assign multiple custom IPS libraries to a group

- 1** In the console, click **Clients**.
- 2** Under View Clients, select the group to which you want to assign the custom signatures.
- 3** On the Policies tab, under Location-independent Policies and Settings, click **Custom Intrusion Prevention**.



- 4 In the Custom Intrusion Prevention for *group name* dialog box, check the check box in the Enabled column for each custom IPS library you want to assign to that group.
- 5 Click **OK**.

## Changing the order of signatures

The IPS engine for custom signatures checks the signatures in the order that they are listed in the signatures list. Only one signature is triggered per packet. When a signature matches an inbound traffic packet or outbound traffic packet, the IPS engine stops checking other signatures. So that the IPS engine executes signatures in the correct order, you can change the order of the signatures in the signatures list. If multiple signatures match, move the higher priority signatures to the top.

For example, if you add a signature group to block TCP traffic in both directions on destination port 80, you might add the following signatures:

- Block all traffic on port 80
- Allow all traffic on port 80

If the Block all traffic signature is listed first, the Allow all traffic signature is never enacted. If the Allow all traffic signature is listed first, the Block all traffic signature is never enacted, and all HTTP traffic is always allowed.

### To change the order of signatures

- 1 Open a custom IPS library.
- 2 Add or edit a signature.  
See [“To add a custom signature”](#) on page 455.
- 3 On the Signatures tab, in the Signatures for this Group table, select the signature that you want to move, and then do one of the following actions:
  - To process this signature before the signature above it, click **Move Up**.
  - To process this signature after the signature below it, click **Move Down**.
- 4 When you finish configuring this library, click **OK**.

## Copying and pasting signatures

You can copy and paste signatures within the same signature group, between signature groups, or between signature libraries. For example, you may realize that you added a signature to the wrong signature group. Or you may want to have two signatures that are nearly identical.

### To copy and paste signatures

- 1 Open a custom IPS library.
- 2 Add or edit a signature.  
See “[To add a custom signature](#)” on page 455.
- 3 In the Custom Intrusion Prevention Signatures dialog box, in the Signatures tab, in the Signatures for this Group table, right-click the signature you want to copy, and then click **Copy**.
- 4 Right-click the signatures list, and then click **Paste**.
- 5 When you finish configuring this library, click **OK**.

## Defining variables for signatures

When you add a custom IPS signature, you can use variables to represent changeable data in signatures. If the data changes, you can edit the variable instead of editing the signatures throughout the library.

Before you can use the variables in the signature, you must define them. The variables you define in the custom signature library can then be used in any signature in that library.

You can copy and paste the content from the existing sample variable to start as a basis for creating content.

### To define variables

- 1 Create a custom IPS library.
- 2 In the Custom Intrusion Prevention Signatures dialog box, click the **Variables** tab.
- 3 Click **Add**.
- 4 In the Add Variable dialog box, type a name and optional description for the variable.
- 5 Add a content string for the variable value of up to 255 characters.  
When you enter the variable content string, follow the same syntax guidelines that you use for entering values into signature content.
- 6 Click **OK**.

After the variable is added to the table, you can use the variable in any signature in the custom library.

**To use variables in signatures**

- 1 On the Signatures tab, add or edit a signature.  
See [“To add a custom signature”](#) on page 455.
- 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**.



# Customizing Network Threat Protection

This chapter includes the following topics:

- [Enabling and disabling Network Threat Protection](#)
- [Configuring Network Threat Protection settings for mixed control](#)
- [Adding hosts and host groups](#)
- [Editing and deleting host groups](#)
- [Adding hosts and host groups to a rule](#)
- [Adding network services](#)
- [Editing and deleting custom network services](#)
- [Adding network services to a rule](#)
- [Enabling network file and printer sharing](#)
- [Adding network adapters](#)
- [Adding network adapters to a rule](#)
- [Editing and deleting custom network adapters](#)
- [Adding applications to a rule](#)
- [Adding schedules to a rule](#)
- [Configuring notifications for Network Threat Protection](#)
- [Setting up network application monitoring](#)

## Enabling and disabling Network Threat Protection

By default, Network Threat Protection is enabled. You may want to disable Network Threat Protection on selected computers. For example, you might need to install a patch on the client computers that would otherwise force the firewall to block the installation.

If you disable Network Threat Protection, it is automatically enabled when the following happens:

- The user shuts down and restarts the client computer.
- The client location changes from server control to client control.
- You configured the client to enable protection after a certain period of time.
- A new security policy that enable protection is downloaded to the client.

You can also manually enable Network Threat Protection from the computer status logs.

See [“Running commands and actions from logs”](#) on page 186.

You can also give the user on the client computer permission to enable or disable protection. However, you can override the client's setting. Or you can disable protection on the client even if users have enabled it. You can enable protection even if users have disabled it.

See [“Configuring user interface settings”](#) on page 108.

### To enable and disable Network Threat Protection for a group

- 1 In the console, click **Clients**.
- 2 Under View Clients, select a group for which you want to enable or disable protection.
- 3 Do one of the following actions:
  - For all computers and users in group, right-click the group, click **Run Command on Group**, and then click **Enable Network Threat Protection** or **Disable Network Threat Protection**.
  - For selected users or computers within a group, on the Clients tab, select the users or computers. Then right-click the selection and click **Run Command on Clients > Enable Network Threat Protection** or **Disable Network Threat Protection**.
- 4 To confirm the action, click **Yes**.
- 5 Click **OK**.

# Configuring Network Threat Protection settings for mixed control

You can set up the client so that users have no control, full control, or limited control over which Network Threat Protection settings they can configure. When you configure the client, use the following guidelines:

- If you set the client to server control, the user cannot create any firewall rules or enable firewall settings and intrusion prevention settings.
- If you set the client to client control, the user can create firewall rules and enable all firewall settings and intrusion prevention settings.
- If you set the client to mixed control, the user can create firewall rules and you decide which firewall settings and intrusion prevention settings the user can enable.

See [“Configuring user interface settings”](#) on page 108.

## To configure Network Threat Protection settings for mixed control

- 1 In the console, click **Clients**.
- 2 Under View Clients, select the group with the user control level you want to modify.
- 3 On the Policies tab, under Location-specific Policies and Settings, under a location, expand **Location-specific Settings**.
- 4 To the right of Client User Interface Control Settings, click **Tasks > Edit Settings**.
- 5 In the Control Mode Settings dialog box, click **Mixed control**, and then click **Customize**.
- 6 On the Client/Server Control Settings tab, under the Firewall Policy category and Intrusion Prevention Policy category, do one of the following actions:
  - To make a client setting available for the users to configure, click **Client**.
  - To configure a client setting, click **Server**.
- 7 Click **OK**.
- 8 For each firewall setting and intrusion prevention setting that you set to Server, enable or disable the setting in the Firewall Policy or Intrusion Prevention Policy.

See [“Enabling Smart traffic filtering”](#) on page 443.

See [“Enabling traffic and stealth settings”](#) on page 444.

See [“Configuring intrusion prevention”](#) on page 449.

## Adding hosts and host groups

A host group is a collection of DNS domain names, DNS host names, IP addresses, IP ranges, MAC addresses, or subnets that are grouped under one name. The purpose of host groups is to eliminate the retyping of host addresses and names. For example, you can add multiple IP addresses one at a time to a firewall rule. Or, you can add multiple IP addresses to a host group, and then add the group to the firewall rule.

As you incorporate host groups, you must describe where the groups are used. If you decide later to delete a host group, you must first remove the host group from all the rules that reference the group.

When you add a host group, it appears at the bottom of the Hosts List. You can access the Hosts list from the Host field in a firewall rule.

See [“About host triggers”](#) on page 429.

### To create host groups

- 1 In the console, click **Policies > Policy Components > Host Groups**.
- 2 Under Tasks, click **Add a Host Group**.
- 3 In the Host Group dialog box, type a name, and then click **Add**.
- 4 In the Host dialog box, in the Type drop-down list, select one of the following hosts:
  - DNS domain
  - DNS host
  - IP address
  - IP range
  - MAC address
  - Subnet
- 5 Enter the appropriate information for each host type.
- 6 Click **OK**.
- 7 Add additional hosts, if necessary.
- 8 Click **OK**.

## Editing and deleting host groups

You can edit or delete any custom host groups that you have added. You cannot edit or delete a default host group. Before you can delete a custom host group,



you must remove the host group from all the rules that reference the group. The settings that you edit change in all rules that reference the group.

#### To edit host groups

- 1 In the console, click **Policies > Policy Components > Host Groups**.
- 2 In the Host Groups pane, select the host group you want to edit.
- 3 Under Tasks, click **Edit the Host Group**.
- 4 In the Host Group dialog box, optionally edit the group name, select a host, and then click **Edit**.

To remove the host from the group, click **Delete**, and then click **Yes**.

- 5 In the Host dialog box, change the host type or edit the host settings.
- 6 Click **OK**.
- 7 Click **OK**.

#### To delete host groups

- 1 In the console, click **Policies > Policy Components > Host Groups**.
- 2 In the Host Groups pane, select the host group you want to delete.
- 3 Under Tasks, click **Delete the Host Group**.
- 4 When you are asked to confirm, click **Delete**.

## Adding hosts and host groups to a rule

To block traffic to or from a specific server, block the traffic by IP address rather than by domain name or host name. Otherwise, the user may be able to access the IP address equivalent of the host name.

#### To add hosts and host groups to a rule

- 1 In the console, open a Firewall Policy.  
See [“About editing policies”](#) on page 327.
- 2 On the Firewall Policy page, click **Rules**.
- 3 On the Rules tab, in the Rules list, select the rule you want to edit, right-click the **Host** field, and then click **Edit**.
- 4 In the Host List dialog box, do one of the following actions:
  - Click **Source/Destination**.
  - Click **Local/Remote**.

- 5 In the Source and Destination or Local and Remote tables, do one of the following tasks:
  - To enable a host group that you added through the Policy Components list, go to step 10.
  - To add a host for the selected rule only, click **Add**.
- 6 In the Host dialog box, select a host type from the Type drop-down list, and enter the appropriate information for each host type.

For more details on each option in this dialog box, click **Help**.
- 7 Click **OK**.
- 8 Add additional hosts, if necessary.
- 9 In the Host List dialog box, for each host or host group that you want to trigger the firewall rule, make sure the check box in the Enabled column is checked.
- 10 Click **OK** to return to the Rules list.

## Adding network services

Network services let networked computers send and receive messages, share files, and print. A network service uses one or more protocols or ports to pass through a specific type of traffic. For example, the HTTP service uses ports 80 and 443 in the TCP protocol. You can create a firewall rule that allows or blocks network services.

The network service list eliminates the necessity to retype a protocol and port for each rule that you create. You can select a network service from a default list of commonly used network services. You can then add the network service to the firewall rule. You can also add network services to the default list.

---

**Note:** IPv4 and IPv6 are the two network layer protocols that are used on the Internet. The firewall blocks attacks that travel through IPv4, but not through IPv6. If you install the client on the computers that run Microsoft Vista, the Rules list includes several default rules that block the Ethernet protocol type of IPv6. If you remove the default rules, you must create a rule that blocks IPv6.

---

If you want to allow or block a network service that is not in the default list, you can add it. You need to be familiar with the type of protocol and the ports that it uses.

To add a custom network service that is accessible from any firewall rule, you add it through the Policy Components list.

#### To add a custom network service to the default list

- 1 In the console, click **Policies > Policy Components > Network Services**.
  - 2 Under Tasks, click **Add a Network Service**.
  - 3 Click **Add a Service**.
  - 4 In the Network Service dialog box, type a name for the service, and then click **Add**.
  - 5 From the Protocol drop-down list, select one of the following protocols:
    - TCP
    - UDP
    - ICMP
    - IP
    - Ethernet
- The options change, based on which protocol you select. For more information, click **Help**.
- 6 Fill in the appropriate fields, and then click **OK**.
  - 7 Add one or more additional protocols, as necessary.
  - 8 Click **OK**.

You can add the service to any firewall rule.

## Editing and deleting custom network services

You can edit or delete any custom network services that you have added. You cannot edit or delete a default network service. Before you can delete a custom network service, you must remove it from all the rules that reference the service.

#### To edit custom network services

- 1 In the console, click **Policies > Policy Components > Network Services**.
- 2 In the Network Services pane, select the service that you want to edit.
- 3 Under Tasks, click **Edit the Network Service**.
- 4 In the Network Service dialog box, change the service name, or select the protocol and click **Edit**.

- 5 Change the protocol settings.

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

- 6 Click **OK**.
- 7 Click **OK**.

#### To delete custom network services

- 1 In the console, click **Policies > Policy Components > Network Services**.
- 2 In the Network Service pane, select the service that you want to delete.
- 3 Under Tasks, click **Delete the Network Service**.
- 4 When you are asked to confirm, click **Yes**.

## Adding network services to a rule

You can add a custom network service through a firewall rule. However, that network service is not added to the default list. You cannot access the custom adapter from any other rule.

#### To add network services to a rule

- 1 In the console, open a Firewall Policy.  
See [“About editing policies”](#) on page 327.
- 2 On the Firewall Policy page, click **Rules**.
- 3 On the Rules tab, in the Rules list, select the rule you want to edit, right-click the Service field, and then click **Edit**.
- 4 In the Service List dialog box, check the **Enable** check box for each service that you want to trigger the rule.
- 5 To add an additional service for the selected rule only, click **Add**.
- 6 In the Protocol dialog box, select a protocol from the Protocol drop-down list.
- 7 Fill out the appropriate fields.  
For more information on these options, click **Help**.
- 8 Click **OK**.
- 9 Click **OK**.

## Enabling network file and printer sharing

You can enable the client to either share its files or to browse for shared files and printers on the local network. To prevent network-based attacks, you may want to disable network file and printer sharing.

You enable network file and print sharing by adding firewall rules. The firewall rules allow access to the ports to browse and share files and printers. You create one firewall rule so that the client can share its files. You create a second firewall rule so that the client can browse for other files and printers.

If the client is in client control or mixed control, users on the client can enable these settings automatically by configuring them in Network Threat Protection. In mixed control, a server firewall rule that specifies this type of traffic can override these settings. In server control, these settings are not available on the client.

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

### To enable clients to browse for files and printers

- 1 In the console, open a Firewall Policy.  
See [“About editing policies”](#) on page 327.
- 2 On the Firewall Policy page, click **Rules**.
- 3 Add a blank rule, and in the Name column, type a name for the rule.  
See [“Adding blank rules”](#) on page 436.
- 4 Right-click the Service field, and then click **Edit**.
- 5 In the Service List dialog box, click **Add**.
- 6 In the Protocol dialog box, in the Protocol drop-down list, click **TCP**, and then click **Local/Remote**.
- 7 In the Remote port drop-down list, type **88, 135, 139, 445**
- 8 Click **OK**.
- 9 In the Service List dialog box, click **Add**.
- 10 In the Protocol dialog box, in the Protocol drop-down list, click **UDP**.
- 11 In the Local Port drop-down list, type **137, 138**
- 12 In the Remote Port drop-down list, type **88**
- 13 Click **OK**.
- 14 In the Service List dialog box, make sure the two services are enabled, and then click **OK**.

- 15 On the Rules tab, make sure the Action field is set to **Allow**.
- 16 If you are done with the configuration of the policy, click **OK**.
- 17 If you are prompted, assign the policy to a location.  
See [“Assigning a shared policy”](#) on page 329.

**To enable other computers to browse files on the client**

- 1 In the console, open a Firewall Policy.  
See [“About editing policies”](#) on page 327.
- 2 On the Firewall Policy page, click **Rules**.
- 3 Add a blank rule, and in the Name column, type a name for the rule.  
See [“Adding blank rules”](#) on page 436.
- 4 Right-click the Service field, and then click **Edit**.
- 5 In the Service List dialog box, click **Add**.
- 6 In the Protocol dialog box, in the Protocol drop-down list, click **TCP**, and then click **Local/Remote**.
- 7 In the Local Port drop-down list, type **88, 135, 139, 445**
- 8 Click **OK**.
- 9 In the Service List dialog box, click **Add**.
- 10 In the Protocol dialog box, in the Protocol drop-down list, click **UDP**.
- 11 In the Local Port drop-down list, type **88, 137, 138**
- 12 Click **OK**.
- 13 In the Service List dialog box, make sure the two services are enabled, and then click **OK**.
- 14 On the Rules tab, make sure the Action field is set to **Allow**.
- 15 If you are done with the configuration of the policy, click **OK**.
- 16 If you are prompted, assign the policy to a location.  
See [“Assigning a shared policy”](#) on page 329.

## Adding network adapters

You can apply a separate firewall rule to each network adapter. For example, you may want to block traffic through a VPN at an office location, but not at a home location.

You can select a network adapter from a default list that is shared across Firewall Policies and rules. The most common adapters are included in the default list in the Policy Components list. The common adapters include VPNs, Ethernet, wireless, Cisco, Nortel, and Enterasys adapters. Use the default list so that you do not have to retype each network adapter for every rule you create.

---

**Note:** The client does not filter or detect network traffic from PDA (personal digital assistant) devices.

---

#### To add a custom network adapter to the default list

- 1 In the console, click **Policies > Policy Components > Network Adapters**.
- 2 Under Tasks, click **Add a Network Adapter**.
- 3 In the Network Adapter dialog box, in the Adapter Type drop-down list, select an adapter.
- 4 In the Adapter Name field, optionally type a description.
- 5 In the Adapter Identification text box, type the case-sensitive brand name of the adapter.

To find the brand name of the adapter, open a command line on the client, and then type the following text:

```
ipconfig/all
```

- 6 Click **OK**.

You can then add the adapter to any firewall rule.

## Adding network adapters to a rule

You can add a custom network adapter from a firewall rule. However, that adapter is not added to the shared list. You cannot access the custom adapter from any other rule.

#### To add a network adapter to a rule

- 1 In the console, open a Firewall Policy.  
See [“About editing policies”](#) on page 327.
- 2 On the Firewall Policy page, click **Rules**.
- 3 On the Rules tab, in the Rules list, select the rule you want to edit, right-click the **Adapter** field, and then click **More Adapters**.
- 4 In the Network Adapter dialog box, do one of the following actions:

- To trigger the rule for any adapter, even if it is not listed, click **Apply the rule to all adapters**, and then go to step 8.
  - To trigger the rule for selected adapters, click **Apply the rule to the following adapters**, and then check the check box in the Enabled column for each adapter that you want to trigger the rule.
- 5 To add a custom adapter for the selected rule only, click **Add**.
  - 6 In the Network Adapter dialog box, select the adapter type and type the adapter's brand name in the Adapter Identification text field.
  - 7 Click **OK**.
  - 8 Click **OK**.

## Editing and deleting custom network adapters

You can edit or delete any custom network adapters that you have added. You cannot edit or delete a default network adapter. Before you can delete a custom adapter, you must remove it from all the rules that reference the adapter. The settings that you edit change in all rules that reference the adapter.

### To edit a custom network adapter

- 1 In the console, click **Policies > Policy Components > Network Adapters**.
- 2 In the Network Adapters pane, select the custom adapter you want to edit.
- 3 Under Tasks, click **Edit the Network Adapter**.
- 4 In the Network Adapters dialog box, edit the adapter type, name, or adapter identification text.
- 5 Click **OK**.

### To delete a custom network adapter

- 1 In the console, click **Policies > Policy Components > Network Adapters**.
- 2 In the Network Adapters pane, select the custom adapter you want to delete.
- 3 Under Tasks, click **Delete the Network Adapter**.
- 4 When you are asked to confirm, click **Yes**.

## Adding applications to a rule

You can define information about the applications that clients run and include this information in a firewall rule. For example, you might want to allow old versions of Microsoft Word.



You can define applications in the following ways:

- You can define the characteristics of an application by entering the information manually. If you do not have enough information, you may want to search the learned applications list.
- You can define the characteristics of an application by searching the learned applications list. Applications in the learned applications list are the applications that client computers in your network run.

#### To define applications

- 1 In the console, open a Firewall Policy.  
See [“About editing policies”](#) on page 327.
- 2 On the Firewall Policies page, click **Rules**.
- 3 On the Rules tab, in the Rules list, right-click the **Application** field, and then click **Edit**.
- 4 In the Application List dialog box, click **Add**.
- 5 In the Add Application dialog box, enter one or more of the following fields:
  - Path and file name
  - Description
  - Size, in bytes
  - Date that the application was last changed
  - File fingerprint
- 6 Click **OK**.
- 7 Click **OK**.

#### To search for applications from the learned applications list

- 1 On the Firewall Policies page, click **Rules**.
- 2 On the Rules tab, select a rule, right-click the **Application** field, and then click **Edit**.
- 3 In the Application List dialog box, click **Add From**.
- 4 In the Search for Applications dialog box, search for an application.  
See [“Searching for applications”](#) on page 346.
- 5 Under the Query Results table, to add the application to the Applications list, select the application, click **Add**, and then click **OK**.

- 6 Click **Close**.
- 7 Click **OK**.

## Adding schedules to a rule

You can set up a time period when a rule is active or not active.

### To add schedules to a rule

- 1 In the console, open a Firewall Policy.  
See [“About editing policies”](#) on page 327.
- 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, click **Add**.
- 5 In the Add Schedule dialog box, configure the start time and end time that you want the rule to be active or not active.
- 6 In the Month drop-down list, select either **All** or a specific month.
- 7 Check one of the following check boxes:
  - Every day
  - Weekends
  - Weekdays
  - Specify days  
If you check Specify days, check one or more of the listed days.
- 8 Click **OK**.
- 9 In the Schedule List, do one of the following actions:
  - To keep the rule active during this time, uncheck the check box in the Any Time Except column.
  - To make the rule inactive during this time, check the check box in the Any Time Except column.
- 10 Click **OK**.

# Configuring notifications for Network Threat Protection

By default, notifications appear on client computers when the client detects various Network Threat Protection events. You can enable some of these notifications. Enabled notifications display a standard message. You can add customized text to the standard message.

Table 34-1 displays the types of events that you can enable and configure.

**Table 34-1** Network Threat Protection notifications

Notification type	Notification type	Description
Display notification on the computer when the client blocks an application	Firewall	A firewall rule on the client blocks an application. You can enable or disable this notification and add additional text to the notification.
Additional text to display if the action for a firewall rule is 'Ask'	Firewall	The applications on the client try to access the network. This notification is always enabled and can't be disabled.
Display Intrusion Prevention notifications	Intrusion prevention	The client detects an intrusion prevention attack. You can enable or disable this notification in server control or mixed control.

### To configure firewall notifications

- 1 In the console, open a Firewall Policy.  
See [“About editing policies”](#) on page 327.
- 2 On the Firewall Policy page, click **Rules**, and then click **Notifications**.
- 3 On the Notifications tab, check **Display notification on the computer when the client blocks an application**.
- 4 To add customized text to the standard message that appears when a rule's action is set to Ask, check **Additional text to display if the action for a firewall rule is 'Ask'**.
- 5 For either notification, click **Set Additional Text**.
- 6 In the Enter Additional Text dialog box, type the additional text you want the notification to display, and then click **OK**.
- 7 When you are done with the configuration of this policy, click **OK**.

### To configure intrusion prevention notifications

- 1 In the console, click **Clients** and under View Clients, select a group.
- 2 On the Policies tab, under Location-specific Policies and Settings, under a location, expand **Location-specific Settings**.
- 3 To the right of Client User Interface Control Settings, click **Tasks > Edit Settings**.
- 4 In the Client User Interface Control Settings for *group name* dialog box, click either **Mixed control** or **Server control**.
- 5 Beside Mixed control or Server control, click **Customize**.  
If you click Mixed control, on the Client/Server Control Settings tab, beside Show/Hide Intrusion Prevention notifications, click **Server**. Then click the **Client User Interface Settings** tab.
- 6 In the Client User Interface Settings dialog box or tab, click **Display Intrusion Prevention notifications**.
- 7 To enable a beep when the notification appears, click **Use sound when notifying users**.
- 8 In the Number of seconds to display notifications text field, type the number of seconds that you want the notification to appear.
- 9 To add text to the standard notification that appears, click **Additional Text**.
- 10 In the Additional Text dialog box, type the additional text you want the notification to display, and then click **OK**.
- 11 Click **OK**.
- 12 Click **OK**.

## Configuring email messages for traffic events

You can configure the Symantec Endpoint Protection Manager to send an email message to you each time the firewall detects a rule violation, attack, or event. For example, you may want to know when a client blocks the traffic that comes from a particular IP address.

### To configure email messages for traffic events

- 1 In the console, open a Firewall Policy.  
See [“About editing policies”](#) on page 327.
- 2 On the Firewall Policy page, click **Rules**.
- 3 On the Rules tab, select a rule, right-click the **Logging** field, and do the following actions:

- To send an email message when a firewall rule is triggered, check **Send Email Alert**.
  - To generate a log event when a firewall rule is triggered, check both **Write to Traffic Log** and **Write to Packet Log**.
- 4 When you are done with the configuration of this policy, click **OK**.
  - 5 Configure a security alert.  
See [“Creating administrator notifications”](#) on page 195.
  - 6 Configure a mail server.  
See [“Establishing communication between Symantec Endpoint Protection Manager and email servers”](#) on page 243.

## Setting up network application monitoring

You can configure the client to detect and monitor any application that runs on the client computer and that is networked. Network applications send and receive traffic. The client detects whether an application's content changes.

An application's content changes for the following reasons:

- A Trojan horse attacked the application.
- The application was updated with a new version or an update.

If you suspect that a Trojan horse has attacked an application, you can use network application monitoring to configure the client to block the application. You can also configure the client to ask users whether to allow or block the application.

Network application monitoring tracks an application's behavior in the Security Log. If an application's content is modified too frequently, it is likely that a Trojan horse attacked the application and the client computer is not safe. If an application's content is modified on an infrequent basis, it is likely that a patch was installed and the client computer is safe. You can use this information to create a firewall rule that allows or blocks an application.

You can add applications to a list so that the client does not monitor them. You may want to exclude the applications that you think are safe from a Trojan horse attack, but that have frequent and automatic patch updates.

You may want to disable network application monitoring if you are confident that the client computers receive adequate protection from Antivirus and Antispyware Protection. You may also want to minimize the number of notifications that ask users to allow or block a network application.

### To set up network application monitoring

- 1 In the console, click **Clients**.
- 2 Under View Clients, select a group, and then click **Policies**.
- 3 On the Policies tab, under Location-independent Policies and Settings, click **Network Application Monitoring**.
- 4 In the Network Application Monitoring for *group name* dialog box, click **Enable Network Application Monitoring**.
- 5 In the **When an application change is detected** drop-down list, select the action that the firewall takes on the application that runs on the client:
  - **Ask**  
Asks the user to allow or block the application.
  - **Block the traffic**  
Blocks the application from running.
  - **Allow and Log**  
Allows the application to run and records the information in the Security Log.  
The firewall takes this action on the applications that have been modified only.
- 6 If you selected Ask, click **Additional Text**.
- 7 In the Additional Text dialog box, type the text that you want to appear under the standard message, and then click **OK**.
- 8 To exclude an application from being monitored, under Unmonitored Application List, do one of the following actions:
  - To define an application manually, click **Add**, fill out one or more fields, and then click **OK**.
  - To define an application from a learned applications list, click **Add From**.  
See [“Searching for applications”](#) on page 346.  
The learned applications feature must be enabled.  
See [“Enabling learned applications”](#) on page 344.

The learned applications list monitors both networked and non-networked applications. You must select networked applications only from the learned applications list. After you have added applications to the Unmonitored Applications List, you can enable, disable, edit, or delete them.
- 9 To enable or disable an application, check the check box in the Enabled column.
- 10 Click **OK**.

# Configuring Proactive Threat Protection

- [Configuring TruScan proactive threat scans](#)
- [Configuring Application and Device Control](#)
- [Setting up hardware devices](#)
- [Customizing Application and Device Control Policies](#)





# Configuring TruScan proactive threat scans

This chapter includes the following topics:

- [About TruScan proactive threat scans](#)
- [About using the Symantec default settings](#)
- [About the processes that TruScan proactive threat scans detect](#)
- [About managing false positives detected by TruScan proactive threat scans](#)
- [About the processes that TruScan proactive threat scans ignore](#)
- [How TruScan proactive threat scans work with Quarantine](#)
- [How TruScan proactive threat scans work with centralized exceptions](#)
- [Understanding TruScan proactive threat detections](#)
- [Configuring the TruScan proactive threat scan frequency](#)
- [Configuring notifications for TruScan proactive threat scans](#)

## About TruScan proactive threat scans

TruScan proactive threat scans provide an additional level of protection to your computer. Proactive threat scans complement your existing antivirus, antispysware, intrusion prevention, and firewall protection technologies.

---

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

---

Antivirus and antispyware scans rely mostly on signatures to detect known threats. Proactive threat scans use heuristics to detect unknown threats. Heuristic process scans analyze the behavior of an application or a process. The scan determines if the process exhibits characteristics of threats, such as Trojan horses, worms, or keyloggers. This type of protection is sometimes referred to as protection from zero-day attacks.

---

**Note:** Auto-Protect also uses a type of heuristic called Bloodhound to detect suspicious behavior in files. Proactive threat scans detect suspicious behavior in active processes.

---

You include settings about proactive threat scans as part of an Antivirus and Antispyware Policy. Many of the settings can be locked so that users on client computers cannot change the settings.

You can configure the following settings:

- What types of threats to scan for
- How often to run proactive threat scans
- Whether or not notifications should appear on the client computer when a proactive threat detection occurs

TruScan proactive threat scans are enabled when both the Scan for Trojan horses and worms or Scan for keyloggers settings are enabled. If either setting is disabled, the Status page in the Symantec Endpoint Protection client shows Proactive Threat Protection as disabled.

Proactive threat scanning is enabled by default.

---

**Note:** Since proactive threat scans analyze applications and processes for behavior anomalies, they can impact your computer's performance.

---

## About using the Symantec default settings

You can decide how you want to manage proactive threat detections. You can use the Symantec defaults, or you can specify the sensitivity level and the detection action.

If you choose to allow Symantec to manage the detections, the client software determines the action and the sensitivity level. The scan engine that runs on the client computer determines the default setting. If you choose to manage the detections instead, you can set a single detection action and a specific sensitivity level.

To minimize false positive detections, Symantec recommends that you use the Symantec-managed defaults initially. After a certain length of time, you can observe the number of false positives that the clients detect. If the number is low, you might want to tune the proactive threat scan settings gradually. For example, for detection of Trojan horses and worms, you might want to move the sensitivity slider slightly higher than its default. You can observe the results of the proactive threat scans that run after you set the new configuration.

See [“Understanding TruScan proactive threat detections”](#) on page 490.

See [“Specifying the actions and sensitivity levels for detecting Trojan horses, worms, and keyloggers”](#) on page 491.

## About the processes that TruScan proactive threat scans detect

Proactive threat scans detect the processes that behave similarly to Trojan horses, worms, or keyloggers. The processes typically exhibit a type of behavior that a threat can exploit, such as opening a port on a user's computer.

You can configure settings for some types of proactive threat detections. You can enable or disable the detection of processes that behave like Trojan horses, worms, or keyloggers. For example, you might want to detect the processes that behave like Trojan horses and worms, but not processes that behave like keylogger applications.

Symantec maintains a list of commercial applications that could be used for malicious purposes. The list includes the commercial applications that record user keystrokes. It also includes the applications that control a client computer remotely. You might want to know if these types of applications are installed on client computers. By default, proactive threat scans detect these applications and log the event. You can specify different remediation actions.

You can configure the type of remediation action that the client takes when it detects particular types of commercial applications. The detections include the commercial applications that monitor or record a user's keystrokes or control a user's computer remotely. If a scan detects a commercial keylogger or a commercial remote control program, the client uses the action that is set in the policy. You can also allow the user to control the actions.

Proactive threat scans also detect the processes that behave similarly to adware and spyware. You cannot configure how proactive threat scans handle these types of detections. If proactive threat scans detect the adware or the spyware that you want to allow on your client computers, you should create a centralized exception.

See [“Configuring a Centralized Exceptions Policy”](#) on page 534.

[Table 35-1](#) describes the processes that proactive threat scans detect.

**Table 35-1** Processes detected by TruScan proactive threat scans

Type of processes	Description
Trojan horses and worms	Processes that exhibit the characteristics of Trojan horses or worms.  Proactive threat scans use heuristics to look for the processes that behave like Trojan horses or worms. These processes may or may not be threats.
Keyloggers	Processes that exhibit the characteristics of keyloggers.  Proactive threat scans detect commercial keyloggers, but they also detect any unknown processes that exhibit keylogger behavior. Keyloggers are the keystroke logging applications that capture users' keystrokes. These applications can be used to gather information about passwords and other vital information. They may or may not be threats.
Commercial applications	Known commercial applications that might be used for malicious purposes.  Proactive threat scans detect several different types of commercial applications. You can configure actions for two types: keyloggers and remote control programs.
Adware and spyware	Processes that exhibit the characteristics of adware and spyware  Proactive threat scans uses heuristics to detect the unknown processes that behave like adware and spyware. These processes may or may not be risks.

You can configure whether or not the client software sends information about proactive threat detections to Symantec. You include this setting as part of an Antivirus and Antispyware Policy.

See [“Submitting information about scans to Symantec”](#) on page 387.

## About managing false positives detected by TruScan proactive threat scans

TruScan proactive threat scans sometimes return false positives. Proactive threat scans look for applications and processes with suspicious behavior rather than known viruses or security risks. By their nature, these scans typically flag the items that you might not want to detect.

For the detection of Trojan horses, worms, or keyloggers, you can choose to use the default action and sensitivity levels that Symantec specifies. Or you can choose to manage the detection actions and sensitivity levels yourself. If you manage the settings yourself, you risk the detection of many false positives. If you want to manage the actions and sensitivity levels, you should be aware of the impact on your security network.

---

**Note:** If you change the sensitivity level, you change the total number of detections. If you change the sensitivity level, you might reduce the number of false positives that proactive threat scans produce. Symantec recommends that if you change the sensitivity levels, you change them gradually and monitor the results.

---

If a proactive threat scan detects a process that you determine is not a problem, you can create an exception. An exception ensures that future scans do not flag the process. Users on client computers can also create exceptions. If there is a conflict between a user-defined exception and an administrator-defined exception, the administrator-defined exception takes precedence.

See [“Configuring a Centralized Exceptions Policy”](#) on page 534.

[Table 35-2](#) outlines the tasks for creating a plan to manage false positives.

**Table 35-2** Plan for managing false positives

Task	Description
<p>Ensure that Symantec manages Trojan horse, worm, and keylogger detections.</p>	<p>Antivirus and Antispyware Policies include the Symantec-managed settings. The setting is enabled by default. When this setting is enabled, Symantec determines the actions that are taken for the detections of these types of processes. Symantec also determines the sensitivity level that is used to scan for them.</p> <p>When Symantec manages the detections, proactive threat scans perform an action that is based on how the scan interprets the detection.</p> <p>The scan applies one of the following actions to the detection:</p> <ul style="list-style-type: none"> <li>■ Quarantine The scan uses this action for the detections that are likely to be true threats.</li> <li>■ Log only The scan uses this action for the detections that are likely to be false positives.</li> </ul> <p><b>Note:</b> If you choose to manage the detection action, you choose one action. That action is always used for that detection type. If you set the action to Quarantine, the client quarantines all detections of that type.</p>
<p>Ensure that Symantec content is current.</p>	<p>Verify that the computers that produce false positives have the latest Symantec content. The latest content includes information about processes that Symantec has determined to be known false positives. These known false positives are excluded from proactive threat scan detection.</p> <p>You can run a report in the console to check which computers are running the latest version of the content.</p> <p>See <a href="#">“About using Monitors and Reports to help secure your network”</a> on page 201.</p> <p>You can update the content by doing any of the following actions:</p> <ul style="list-style-type: none"> <li>■ Apply a LiveUpdate Policy. See <a href="#">“Configuring LiveUpdate Policies”</a> on page 92.</li> <li>■ Run the Update command for the selected computers that are listed on the Clients tab.</li> <li>■ Run the Update command on the selected computers that are listed in the computer status or risk log</li> </ul>

**Table 35-2** Plan for managing false positives (*continued*)

Task	Description
Make sure that submissions are enabled.	<p>Submissions settings are included as part of the Antivirus and Antispyware Policy.</p> <p>Make sure that client computers are configured to automatically send information to Symantec Security Response about processes detected by proactive threat scans. The setting is enabled by default.</p> <p>See <a href="#">“Submitting information about scans to Symantec”</a> on page 387.</p>
Create exceptions for the false positives that you discover.	<p>You can create a policy that includes exceptions for the false positives that you discover. For example, you might run a certain process or application in your security network. You know that the process is safe to run in your environment. If TruScan proactive threat scans detect the process, you can create an exception so that future scans do not detect the process.</p> <p>See <a href="#">“Configuring a Centralized Exceptions Policy”</a> on page 534.</p>

## About the processes that TruScan proactive threat scans ignore

TruScan proactive threat scans allow certain processes and exempt those processes from the scans. Symantec maintains this list of processes. Symantec typically populates the list with the applications that are known false positives. The client computers in your security network receive updates to the list periodically when they download new content. The client computers can download the content in several ways. The management server can send updated content. You or your users can also run LiveUpdate on the client computers.

TruScan proactive threat scans ignore some processes. These processes might include the applications for which Symantec does not have enough information or the applications that load other modules.

You can also specify that TruScan proactive threat scans ignore certain processes. You specify that proactive threat scans ignore certain processes by creating a centralized exception.

Users on client computers can also create exceptions for proactive threat scans. If an administrator-defined exception conflicts with a user-defined exception, proactive threat scans apply only the administrator-defined exception. The scan ignores the user exception.

See [“How TruScan proactive threat scans work with centralized exceptions”](#) on page 488.

## How TruScan proactive threat scans work with Quarantine

You can configure proactive threat scans to quarantine detections. Users on client computers can restore quarantined items. The Symantec Endpoint Protection client can also restore quarantined items automatically.

When a client receives new definitions, the client rescans quarantined items. If the quarantined items are considered malicious, the client logs the event.

Periodically, client computers receive updates to Symantec-defined lists of known good processes and applications. When new lists are available on client computers, quarantined items are checked against the latest lists. If the latest lists permit any of the quarantined items, the client automatically restores the items.

In addition, administrators or users might create exceptions for proactive threat detections. When the latest exceptions permit the quarantined items, the client restores the items.

Users can view the quarantined items on the View Quarantine page in the client.

The client does not submit the items that proactive threat scans quarantine to a central Quarantine Server. Users can automatically or manually submit items in the local Quarantine to Symantec Security Response.

See [“Submitting quarantined items to Symantec”](#) on page 393.

## How TruScan proactive threat scans work with centralized exceptions

You can create your own exception lists for the Symantec Endpoint Protection client to check when it runs proactive threat scans. You create these lists by creating exceptions. The exceptions specify the process and the action to take when a proactive threat scan detects a specified process. You can only create exceptions for the processes that are not included in the Symantec-defined list of known processes and applications.

For example, you might want to create an exception to do any of the following:

- Ignore a certain commercial keylogger
- Quarantine a particular application that you do not want to run on client computers



- Allow a specific remote control application to run

To avoid conflicts between exceptions, proactive threat scans use the following order of precedence:

- Symantec-defined exceptions
- Administrator-defined exceptions
- User-defined exceptions

The Symantec-defined list always takes precedence over administrator-defined exceptions. Administrator-defined exceptions always take precedence over user-defined exceptions.

You can use a centralized exceptions policy to specify that known, detected processes are allowed by setting the detection action to Ignore. You can also create a centralized exception to specify that certain processes are not permitted by setting the action to Quarantine or Terminate.

Administrators can force a proactive threat detection by creating a centralized exception that specifies a file name for proactive threat scans to detect. When the proactive threat scan detects the file, the client logs the instance. Because file names are not unique, multiple processes might use the same file name. You can use forced detections to help you create exceptions to ignore, quarantine, or terminate a particular process.

When a proactive threat scan on the client computer logs the detection, the detection becomes part of a list of known processes. You can select from the list when you create an exception for proactive threat scans. You can set a particular action for the detection. You can also use the proactive detection log under the Monitors tab in the console to create the exception.

See [“Configuring a Centralized Exceptions Policy”](#) on page 534.

See [“Viewing logs”](#) on page 180.

Users can create exceptions on the client computer through one of the following methods:

- The View Quarantine list
- The scan results dialog box
- Centralized exceptions

An administrator can lock an exceptions list so that a user cannot create any exceptions. If a user previously created exceptions before the administrator locked the list, the user-created exceptions are disabled.

# Understanding TruScan proactive threat detections

When a TruScan proactive threat scan detects processes that it flags as potentially malicious, typically some of the processes are legitimate processes. Some detections do not provide enough information to be categorized as a threat or a false positive; these processes are considered "unknown."

A proactive threat scan looks at the behavior of active processes at the time that the scan runs. The scan engine looks for behavior such as opening ports or capturing keystrokes. If a process involves enough of these types of behaviors, the scan flags the process as a potential threat. The scan does not flag the process if the process does not exhibit suspicious behavior during the scan.

By default, proactive threat scans detect the processes that behave like Trojan horses and worms or processes that behave like keyloggers. You can enable or disable these types of detections in an Antivirus and Antispyware Policy.

---

**Note:** Proactive threat scan settings have no effect on antivirus and antispyware scans, which use signatures to detect known risks. The client detects known risks first.

---

The client uses Symantec default settings to determine what action to take on the detected items. If the scan engine determines that the item does not need to be remediated, the client logs the detection. If the scan engine determines that the item should be remediated, the client quarantines the item.

---

**Note:** The Scan for trojans or worms and the Scan for keyloggers options are currently not supported on Windows server operating systems. You can modify the options in the Antivirus and Antispyware Policy for the clients that run on server operating systems, but the scans do not run. In the client user interface on server operating systems, the scanning options appear unavailable. If you enable the scanning options in the policy, the options appear checked and unavailable.

---

Symantec default settings are also used to determine the sensitivity of the proactive threat scan. When the sensitivity level is higher, more processes are flagged. When the sensitivity level is lower, fewer processes are flagged. The sensitivity level does not indicate the level of certainty about the detection. It also does not affect the rate of false positive detections. The higher the sensitivity level, the more false positives and true positives the scan detects.

You should use the Symantec default settings to help minimize the number of false positives that you detect.

You can disable the Symantec-defined default settings. When you disable the Symantec default settings, you can configure actions and the sensitivity level for the detection of Trojan horses, worms, or keyloggers. In the client user interface, the default settings that appear do not reflect the Symantec default settings. They reflect the default settings that are used when you manually manage detections.

For commercial applications, you can specify the action that the client takes when a proactive threat scan makes a detection. You can specify separate actions for the detection of a commercial keylogger and the detection of a commercial remote control application.

---

**Note:** Users on client computers can modify the proactive threat scan settings if the settings are unlocked in the Antivirus and Antispyware Policy. On the client computer, the TruScan proactive threat scan settings appear under Proactive Threat Protection.

---

## Specifying the types of processes that TruScan proactive threat scans detect

By default, TruScan proactive threat scans detect Trojan horses, worms, and keyloggers. You can disable the detection of Trojan horses and worms, or keyloggers.

You can click [Help](#) for more information about the scan's process type options.

### To specify the types of processes that TruScan proactive threat scans detect

- 1 On the Antivirus and Antispyware Policy page, click **TruScan Proactive Threat Scans**.
- 2 On the Scan Details tab, under Scanning, check or uncheck **Scan for trojans and worms** and **Scan for keyloggers**.
- 3 Click **OK**.

## Specifying the actions and sensitivity levels for detecting Trojan horses, worms, and keyloggers

TruScan proactive threat scans differ from antivirus and antispyware scans. Antivirus and antispyware scans look for known risks. Proactive threat scans look for unknown risks based on the behavior of certain types of processes or applications. The scans detect any behavior that is similar to the behavior of Trojan horses, worms, or keyloggers.

When you let Symantec manage the detections, the detection action is Quarantine for true positives and Log only for false positives.

When you manage the detections yourself, you can configure the detection action. That action is always used when proactive threat scans make a detection. For example, you might specify that the Symantec Endpoint Protection client logs the detection of processes that behave like Trojan horses and worms. When the client makes a detection, it does not quarantine the process, it only logs the event.

You can configure the sensitivity level. Proactive threat scans make more detections (true positives and false positives) when you set the sensitivity level higher.

---

**Note:** If you enable these settings, you risk detecting many false positives. You should be aware of the types of processes that you run in your security network.

---

You can click Help for more information about the scan's action and sensitivity options.

**To specify the action and sensitivity for Trojan horses, worms, or keyloggers**

- 1 On the Antivirus and Antispyware Policy page, click **TruScan Proactive Threat Scans**.
- 2 On the Scan Details tab, under Scanning, make sure that you check **Scan for trojans and worms** and **Scan for keyloggers**
- 3 For either risk type, uncheck **Use defaults defined by Symantec**.
- 4 For either risk type, set the action to Log, Terminate, or Quarantine.

Notifications are sent if an action is set to Quarantine or Terminate, and you have enabled notifications. (Notifications are enabled by default.) Use the Terminate action with caution. In some cases, you can cause an application to lose functionality.

- 5 Do one of the following actions:
  - Move the slider to the left or right to decrease or increase the sensitivity, respectively.
  - Click **Low** or **High**.
- 6 Click **OK**.

## Specifying actions for commercial application detections

You can change the action that is taken when a TruScan proactive threat scan makes a detection. If you set the action to Ignore, proactive threat scans ignore commercial applications.

You can click Help for more information about the options that are used in procedures.

#### To specify actions for commercial application detections

- 1 On the Antivirus and Antispyware Policy page, click **TruScan Proactive Threat Scans**.
- 2 On the Scan Details tab, under Detecting Commercial Applications, set the action to Ignore, Log, Terminate, or Quarantine.
- 3 Click **OK**.

## Configuring the TruScan proactive threat scan frequency

You can configure how often TruScan proactive threat scans run by including the setting in an Antivirus and Antispyware Policy.

---

**Note:** If you change the frequency of proactive threat scans, it can impact the performance of client computers.

---

You can click Help for more information about the scan's frequency options.

#### To configure the proactive threat scan frequency

- 1 On the Antivirus and Antispyware Policy page, click **TruScan Proactive Threat Scans**.
- 2 On the Scan Frequency tab, under Scan Frequency, set one of the following options:
  - At the default scanning frequency  
The scan engine software determines the scan frequency. This option is the default setting.
  - At a custom scanning frequency  
If you enable this option, you can specify that the client scans new processes immediately when it detects them. You can also configure the scan frequency time.
- 3 Click **OK**.

# Configuring notifications for TruScan proactive threat scans

By default, notifications are sent to client computers whenever there is a TruScan proactive threat scan detection. You can disable notifications if you do not want the user to be notified.

Notifications alert the user that a proactive threat scan made a detection that the user should remediate. The user can use the notification dialog box to remediate the detection. For the proactive threat scan detections that do not require remediation, the Symantec Endpoint Protection client logs the detection but does not send a notification.

---

**Note:** If you set the detections to use the Symantec default settings, notifications are sent only if the client recommends a remediation for the process.

---

Users can also remediate detections by viewing the Threat log and by selecting an action.

You can create a centralized exception to exclude a process from detection; users on client computers can also create exceptions.

See [“About Centralized Exceptions Policies”](#) on page 531.

You can click Help for more information about the scan's notification options.

## To configure notifications for TruScan proactive threat scans

- 1 On the Antivirus and Antispyware Policy page, click **TruScan Proactive Threat Scans**.
- 2 On the Notifications tab, check or uncheck the following options:
  - Display a message when there is a detection.
  - Prompt before terminating a process.
  - Prompt before stopping a service.
- 3 Click **OK**.

# Configuring Application and Device Control

This chapter includes the following topics:

- [About application and device control](#)
- [About the structure of an Application and Device Control Policy](#)
- [About application control](#)
- [About device control](#)
- [About working with Application and Device Control Policies](#)
- [Enabling a default application control rule set](#)
- [Creating an Application and Device Control Policy](#)
- [Configuring application control for an Application and Device Control Policy](#)
- [Configuring device control for an Application and Device Control Policy](#)

## About application and device control

You might want to use application and device control for the following reasons:

- To prevent malware from hijacking applications on client computers
- To prevent the inadvertent removal of data from client computers
- To restrict the applications that can run on a client computer
- To minimize the possibility of a computer being infected with security threats from a peripheral device

Application and device control is implemented on client computers using an Application and Device Control Policy.

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

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

You can define each of these two types of protection when you create a new Application and Device Control Policy. You also have the option to add either application control or device control first and then the other type of protection at a later time.

You can apply only one Application and Device Control Policy to each location within a group. You must define both application control and device control in the same policy if you want to implement both types of protection.

---

**Note:** The information in this chapter applies only to 32-bit client computers. Application and Device Control Policies do not work on 64-bit client computers.

---

## About the structure of an Application and Device Control Policy

The application control portion of an Application and Device Control Policy can contain multiple rule sets, and each rule set contains one or more rules. You can configure properties for a rule set, and properties, conditions, and actions for each rule.

Rules control attempts to access computer entities, such as files or registry keys, that Symantec Endpoint Protection monitors. You configure these different types of attempts as conditions. For each conditions, you can configure actions to take when the conditions are met. You configure rules to apply to only certain applications, and you can optionally configure them to exclude other applications from having the action applied.

See [“About application control rule properties”](#) on page 499.

See [“About application control rule conditions”](#) on page 499.

See [“About application control rule condition properties”](#) on page 500.

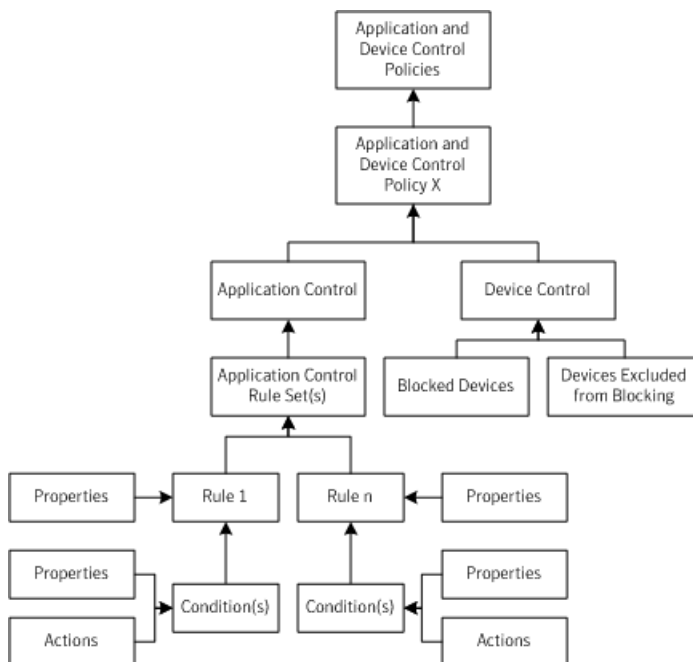
See [“About application control rule condition actions”](#) on page 500.



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 36-1 illustrates the application and device control components and how they relate to each other.

**Figure 36-1** Application and Device Control Policy structure



## About application control

Application control provides the ability to monitor and to control the behavior of applications. You can block or allow access to specified registry keys, files, and folders. You can also block or allow applications to launch or terminate other processes. You can define which applications are permitted to run and which applications cannot be terminated through irregular processes. You can define which applications can call Dynamic Link Libraries (DLLs).

---

**Warning:** Application control is an advanced security feature that only experienced administrators should configure.

---

Application control is implemented by using sets of rules that define how you want to control the applications. Application control is a set of controls that allow or block an action. You can create as many rule sets as you need in a policy. You can also configure which rule sets are active at any given time by using the Enabled option for each rule set.

You can use application control to protect client computers in the following ways:

- Protect specific registry keys and values.
- Safeguard directories such as the \WINDOWS\system directory.
- Prevent users from altering configuration files.
- Shield important program files such as the Symantec home directory where the client is installed.
- Protect specific processes or exclude processes from protection.
- Control access to DLLs.

## About Test mode

When you create an application control rule set, you create it in the default mode, which is Test (log only) mode. Test mode lets you test your rules before you enable them. In Test mode, no actions are applied, but the actions that you have configured are logged as if they had been applied. Using Test mode, you can assign the policy to groups and locations and generate a client Control log. Examine the client Control logs for errors and make corrections to the rule as necessary. When the policy operates as you expect it to, you can change the mode to Production mode to implement the application control rule set.

A best practice is to run all rule sets in Test mode for a period of time before you switch them to Production mode. This practice reduces the potential for the problems that can occur when you do not anticipate all the possible ramifications of a rule.

See [“Changing the mode of an application control rule set”](#) on page 513.

## About application control rule sets and rules

Rule sets consist of rules and their conditions. A rule is a set of conditions and actions that apply to a given process or processes. A best practice is to create one rule set that includes all of the actions that allow, block, and monitor one given task. Follow this principle to help to keep your rules organized. For example, suppose you want to block write attempts to all removable drives and you want to block applications from tampering with a particular application. To accomplish

these goals, you should create two different rule sets. You should not create all of the necessary rules to accomplish both these goals with one rule set.

You apply a rule to one or more applications to define the applications that you monitor. Rules contain conditions. These conditions monitor the application or applications that are defined in the rule for specified operations. Conditions define what you want to allow the applications to do or to keep them from doing. Conditions also contain the actions to take when the operation that is specified in the condition is observed.

---

**Note:** Remember that actions always apply to the process that is defined in the rule. They do not apply to the processes that are defined in the condition.

---

## About application control rule properties

You can configure the following properties for a rule:

- A name
- A description (optional)
- Whether the rule is enabled or disabled
- A list of the applications that should have the rule applied to them
- A list of the applications that should not have the rule applied to them (optional)

## About application control rule conditions

Conditions are the operations that can be allowed or denied for applications.

[Table 36-1](#) describes the application control rule conditions that you can configure for a rule.

**Table 36-1** Types of rule conditions

Condition	Description
Registry Access Attempts	Allow or block access to a client computer's registry settings. You can allow or block access to specific registry keys, values, and data.
File and Folder Access Attempts	Allow or block access to specified files or folders on a client computer. You can restrict the monitoring of files and folders to specific drive types.

**Table 36-1** Types of rule conditions (*continued*)

Condition	Description
Launch Process Attempts	Allow or block the ability to launch a process on a client computer.
Terminate Process Attempts	<p>Allow or block the ability to terminate a process on a client computer.</p> <p>For example, you may want to block a particular application from being stopped. This condition looks for the applications that try to kill a specified application.</p> <p><b>Note:</b> This condition prevents other applications or procedures from terminating the process. It does not prevent application termination by the usual methods of quitting an application, such as clicking Quit from the File Menu.</p>
Load DLL Attempts	<p>Allow or block the ability to load a DLL on a client computer.</p> <p>You can define the DLL files that you want to prevent or allow to be loaded into an application. You can use specific file names, wildcard characters, fingerprint lists, and regular expressions. You can also limit the monitoring of DLLs to those DLLs that are launched from a particular drive type.</p>

## About application control rule condition properties

You can configure the following properties for a rule condition:

- A name
- A description (optional)
- Whether the rule condition is enabled or disabled
- A list of the computer entities that should be monitored for the condition
- A list of the computer entities that should be excluded from monitoring for the condition (optional)

## About application control rule condition actions

You can configure certain actions to be taken when a condition is met.

The following actions can be configured when an application attempt occurs:

- Continue processing other rules.
- Allow the application to access the entity.
- Block the application from accessing the entity.

- Terminate the application process.

For example, you can configure one set of actions to take place when a process tries to read a monitored entity. You can configure a different set of actions to occur when the same process tries to create, delete, or write to a monitored entity. You can configure an action in each case for as many processes as you want.

You can also configure application control to log the attempts and to display a custom message to the user when an attempt has occurred.

---

**Warning:** Use the Terminate process action carefully because it may not have the effect that you expect when you use it in a rule. It terminates the process that is performing the configured action, not the process that the user is currently starting.

---

For example, suppose you want to terminate Winword.exe any time that any process launches Winword.exe. You decide to create a rule, and you configure it with the Launch Process Attempts condition and the Terminate process action. You apply the condition to Winword.exe and apply the rule to all processes. One may expect this rule to terminate Winword.exe, but that is not what a rule with this configuration does. If you try to start Winword.exe from Windows Explorer, a rule with this configuration terminates Explorer.exe, not Winword.exe.

## About device control

Use device control to manage peripheral devices' access to client computers. You can implement device control by constructing Hardware Device Control Lists. You can construct a list of devices that should be blocked from computer access and a list of devices that should be allowed access. Although a device might be physically connected to a computer, the device can still be denied access to that computer. You can block or allow USB, infrared, FireWire, and SCSI devices, as well as serial ports and parallel ports.

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

[Table 36-2](#) lists sample port and device configuration combinations and the effect each combination has on the device that tries to access the client computer.

**Table 36-2** Port and device configuration combinations

Configuration	Result
Port blocked + device excluded	Device works
Port excluded + device blocked	Device does not work <b>Note:</b> You should never block a keyboard.

For example, you may decide to block all ports, but exclude a USB mouse so that it can connect to a client computer. In this scenario, the USB mouse works on the client computer even though that port is blocked.

## About working with Application and Device Control Policies

You create and edit Application and Device Control Policies in the same manner as you create and modify other types of Symantec Endpoint Protection policies. You can assign, withdraw, replace, copy, export, import, or delete an Application and Device Control Policy.

If the default Application and Device Control Policy does not provide the protection you need, you have the following choices:

- Edit the default policy.
- Create a custom policy.

See [“Configuring application control for an Application and Device Control Policy”](#) on page 504.

---

**Warning:** An Application and Device Control Policy is a powerful tool that lets you create custom enforcement policies for your environment. However, configuration errors can disable a computer or a server. The client computer can fail, or its communication with the Symantec Endpoint Protection Manager can be blocked, when you implement an Application and Device Control Policy. If this type of failure occurs, you may not be able to configure the client computer remotely. Your only option may be to restore the client computer locally. Symantec recommends you first use a policy in Test mode before you deploy it. You can then examine the Control log for errors.

---

Application and device control events are recorded in the client's Control log. You can view them on the console in the Application Control log and the Device Control log.

You typically assign a policy to multiple groups in your security network. You can create a non-shared, location-specific policy if you have specific requirements for a particular location.

---

**Note:** The procedures in this chapter assume that you are familiar with the basics of policy configuration.

---

See [“About working with policies”](#) on page 322.

## Enabling a default application control rule set

The application control portion of an Application and Device Control Policy is made up of application control rule sets. Each application control rule set is made up of one or more rules. Default application control rule sets are installed with the Symantec Endpoint Protection Manager. The default rule sets are disabled at installation.

---

**Note:** Do not edit the default application control rule sets. If the default rule sets and controls do not meet your requirements, create a new application control rule set to meet your requirements instead.

---

If you want to use the default rule sets in an Application and Device Control Policy, you must enable them.

### To enable a default application control rule set

- 1 In Application and Device Control Policies, click the policy to which you want to add a default application control rule set.
- 2 Under Tasks, click **Edit the Policy**.
- 3 Click **Application Control**.
- 4 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.
- 5 When you have finished reviewing the rules and their condition settings, click **Cancel**.
- 6 Check the check box next to each rule set that you want to enable.
- 7 Click **OK**.

## Creating an Application and Device Control Policy

You can create a new Application and Device Control Policy. After you create a new policy, you can create one or more application control rule sets, or hardware device control lists, or both.

You should not create one policy that contains only device control and one that contains only application control. An Application and Device Control Policy must contain both application control and device control if you want to implement both. You can only assign one Application and Device Control Policy at a time to a group or a location.

### To create and assign an Application and Device Control Policy

- 1 In the Symantec Endpoint Protection Manager console, click **Policies**.
- 2 Under View Policies, click **Application and Device Control**.
- 3 Under Tasks, click **Add an Application and Device Control Policy**.
- 4 In the Overview pane, in the Policy name field, type the name of the new Application and Device Control Policy.  
The default name for a new policy is New Application and Device Control Policy.
- 5 In the Description field, type a description of the new policy.  
This information is optional; it is used for reference purposes only.
- 6 If you do not want to immediately implement the policy, uncheck **Enable this policy**.  
New policies are enabled by default.
- 7 Click **OK**.

## Configuring application control for an Application and Device Control Policy

To configure application control, you need to accomplish the following tasks:

- Create a new application control rule set.
- Add one or more rules to the rule set.
- Add one or more conditions to the rules.
- Configure the actions to be taken when the conditions are met.
- Apply the conditions to entities.



- Optionally, exclude entities from having the conditions applied to them.
- Apply the rules to processes.
- Optionally, exclude processes from having the rules applied to them.
- Enable the rules.
- Enable the rule set.

## Creating a new application control rule set and adding a new rule to the set

A new application rule set contains one or more administrator-defined rules. Each rule set and each rule has properties. Each rule can also contain one or more conditions for monitoring applications and their access to specified files, folders, registry keys, and processes.

You can create multiple rules and add them to a single application control rule set. Create as many rules and as many rule sets as you need to implement the protection you want. You can delete rules from the rules list and change their position in the rule set hierarchy as needed. You can also enable and disable rule sets or individual rules within a set.

The order in which the rules are listed is important to the functioning of application control. Application control rules work similarly to most network-based firewall rules in that both use the first rule match feature. When there are multiple rules where the conditions are true, the top rule is the only one that is applied unless the action that is configured for the rule is to Continue processing other rules.

You should consider the order of the rules and their conditions when you configure them to avoid unexpected consequences. Consider the following scenario: Suppose an administrator wants to prevent all users from moving, copying, and creating files on USB drives. The administrator has an existing rule with a condition that allows write access to a file named Test.doc. The administrator adds a second condition to this existing rule set to block all USB writes. In this scenario, users are still able to create and modify a Test.doc file on USB drives. Because the Allow writes to Test.doc condition comes before the Block all USB writes in the rule, the Block all USB writes does not get processed when the condition that precedes it in the list is true.

You can review the structure of the default rule sets to see how they are constructed.

---

**Warning:** Only advanced administrators should create application control rule sets.

Configuration errors in the rule sets that are used in an Application and Control Policy can disable a computer or a server. The client computer can fail, or its communication with the Symantec Endpoint Protection Manager can be blocked.

---

**To create a new rule set and add rules to it**

- 1 In the Application Control dialog box, click **Add**.
- 2 Because logging is enabled by default, 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 If you do not want to immediately enable this new rule, uncheck **Enable this rule**.
- 7 To add a second rule, click **Add**, and then click **Add Rule**.
- 8 Click **OK**.

After you create a rule set and a rule, you should define the applications that the rule should apply to. If necessary, you should also define any applications that should be excluded from having the rule applied to them. You can then add conditions to the rule and configure actions to be taken when the conditions are met.

## Adding conditions to a rule

After you apply a rule to at least one application, you can add and configure conditions for the rule. Conditions have properties and actions. A condition's properties specify what the condition looks for. Its actions define what happens when the condition is met.

**To add a condition to a rule**

- 1 In the Application Control pane, click the rule set you created, and then click **Edit**.
- 2 In the Edit Application Control Rule Set dialog box, click the rule to which you want to add a condition.

- 3 Under the Rules list, click **Add**, and then click **Add Condition**.
- 4 Select one of the following conditions:
  - Registry Access Attempts
  - File and Folder Access Attempts
  - Launch Process Attempts
  - Terminate Process Attempts
  - Load DLL Attempts

You can add, configure, and delete conditions from a rule as needed.

## Configuring condition properties for a rule

Condition properties include the name, description, and whether the condition is enabled or disabled. Condition properties also include the application of the condition to entities and optionally, the exclusion of some entities from having the condition applied.

---

**Note:** When you apply a condition to all entities in a particular folder, a best practice is to use *folder\_name\\** or *folder\_name\\*\\**. One asterisk includes all the files and folders in the named folder. Use *folder\_name\\*\\** to include every file and folder in the named folder plus every file and folder in every subfolder.

---

### To configure condition properties

- 1 In the Edit Application Control Rule Set dialog box, click the condition that you want to apply.
- 2 If desired, change the default name in the Name text box, and optionally add a description.
- 3 If you want to immediately enable this condition, check **Enable this condition**.
- 4 To the right of Apply to the following *entity*, where *entity* represents processes, registry keys, files and folders, or DLLs, click **Add**.
- 5 In the Add *entity* Definition dialog box, configure one of the following sets of options:
  - For **Registry Access Attempts**, type the name of the registry key and its value name and data.  
Click either **Use wildcard matching (\* and ? supported)** or **Use regular expression matching**.
  - For **File and Folder Access Attempts**, type the name of the file or folder.

Click either **Use wildcard matching (\* and ? supported)** or **Use regular expression matching**.

If desired, check specific drive types on which to match the files and folders.

If desired, check **Only match 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.

- For **Launch Process Attempts**, type the name of the process.  
Click either **Use wildcard matching (\* and ? supported)** or **Use regular expression matching**.  
If desired, check specific drive types on which to match the process.  
If desired, check **Only match processes running on the following device id type**, and then type a device ID type in the text field or click **Select** to select a device ID type from the list in the Device Selection dialog box to only match the processes that run on devices of that ID type.  
If desired, click **Options** to match processes based on the file fingerprint and to only match the processes that have a designated argument. You can choose to match the arguments exactly or by using regular expression matching.
- For **Terminate Process Attempts** or **DLL Access Attempts**, type the name of the process.  
Click either **Use wildcard matching (\* and ? supported)** or **Use regular expression matching**.  
If desired, check specific drive types on which to match the process.  
If desired, check **Only match processes running on the following device id type**, and then type a device ID type in the text field or click **Select** to select a device ID type from the list in the Device Selection dialog box to only match the processes that run on devices of that ID type.  
If desired, click **Options** to match processes based on the file fingerprint.

6 Click **OK**.

7 To the right of the Do not apply this rule to the following processes pane, click **Add**, and repeat the configuration as desired.

You have the same options for the exclusions as you do for the inclusions.

8 Click the appropriate controls to make your selections, and type any required information into the text boxes.

9 Click **OK**.

After you set properties for the condition, you need to configure the actions that are taken when the condition is met.

## Configuring the actions to take when a condition is met

The following actions are available for all conditions:

Continue processing other rules	Allows you to only log the event and then continue processing other rules in the list  For all other actions, the client computer stops processing rules after the first criterion matches
Allow access	Allows the operation to continue
Block access	Prevents the operation
Terminate Process	Kills the application that has made the request

---

**Note:** A best practice is to use the Block access action to prevent a condition rather than to use the Terminate process action. The Terminate process action should be used only in advanced configurations.

---

### To configure the actions to take when a condition is met

- 1 In the Edit Application Control Rule Set dialog box, click the condition for which you want to configure actions.
- 2 On the Actions tab, do one of the following actions:
  - For the Launch Process Attempts condition and the Terminate Process Attempts condition, click one of the following options: **Continue processing other rules**, **Allow access**, **Block access**, or **Terminate process**.
  - For the DLL Access Attempts condition, click one of the following options: **Continue processing other rules**, **Allow access**, **Block access**, or **Terminate process**.
  - For the Registry Access Attempts condition and the File and Folder Access Attempts condition, you can configure two sets of actions. One set applies when there is a read attempt; the other set applies when there is a create, delete, or write attempt.  
 Under Read Attempt, click one of the following options: **Continue processing other rules**, **Allow access**, **Block access**, or **Terminate process**.
- 3 If desired, check **Enable logging**, and then select a severity level to assign to the entries that are logged.
- 4 If desired, check **Notify user**, and then type the text that you want to user to see.

- 5 Repeat steps 2 through 4 to configure the same options for Create, Delete, or Write Attempts.
- 6 Click **OK**.

## Applying a rule to specific applications and excluding applications from a rule

You can apply a rule to applications, and you can exclude applications from the rule's actions. You specify one list that contains the applications to which the rule applies (the inclusions). You specify another list that contains the applications to which the rule does not apply (the exclusions). To tie a rule to a specific application, you define that application in the Apply this rule to the following processes text field.

If you want to tie the rule to all applications except for a given set of applications, then you can use the following settings:

- In the Apply this rule to the following processes text box, define a wildcard character for all processes (\*).
- In the Do not apply this rule to the following processes text box, list the applications that need an exception.

You can define as many applications as you want for each list.

---

**Note:** Every rule must have at least one application listed in the Apply this rule to the following processes text box.

---

When you add applications to a rule, you can use the following ways to specify the application:

- The process name
- Wildcard characters
- Regular expressions
- File fingerprints
- The drive types from where the application was launched
- The device ID

### To apply a rule to specific applications

- 1 In the Edit Application Control Rule Set dialog box, click the rule that you want to apply.
- 2 If you want to configure an application to apply the rule to, then to the right of Apply this rule to the following processes, click **Add**.
- 3 In the Add Process Definition dialog box, configure the following items:
  - Type the name of the application that you want to match in this rule.
  - Click either **Use wildcard matching (\* and ? supported)** or **Use regular expression matching** for matching the name.
  - If desired, check the specific drive types on which to match the process.
  - If desired, check **Only match processes running on the following device id type**, and then type a device ID type in the text field or click **Select** to select a device ID type from the list in the Device Selection dialog box to only match the processes that run on devices of that ID type.
  - If desired, click **Options** to match processes based on the file fingerprint and to match only the processes that have a designated argument. You can choose to match the arguments exactly or by using regular expression matching.
- 4 Click **OK**.  
 You can repeat steps 2 through 4 to add as many applications as you want.
- 5 If you want to configure one or more applications to exclude from the rule, then to the right of the Do not apply this rule to the following processes text field, click **Add**.  
 Repeat the configuration of the applications to exclude as desired. You have the same options when you define an application to exclude as you have when you apply the rule to an application.
- 6 When you have finished defining the applications, click **OK**.

## Changing the order in which application control rule sets are applied

You can control the order in which application control rule sets are applied. You can also control the order in which individual rules within a rule set are applied.

### To change the order in which application control rule sets are applied

- 1 In the console, click **Policies**.
- 2 In the View Policies pane, click **Application and Device Control**.
- 3 Click the policy that you want to edit.

- 4 Under Tasks, click **Edit the Policy**.
- 5 Click **Application Control**.
- 6 Click the application control rule set that you want to move.
- 7 Click **Move Up** or **Move Down** to change its priority within the list.
- 8 Repeat the previous two steps for each rule set that you want to reprioritize.
- 9 Click **OK**.

## Disabling application control rule sets and individual rules in an Application and Device Control Policy

You may need to disable a particular application control rule set in an Application and Device Control Policy without withdrawing or deleting the entire policy.

### To disable an application control rule set in an Application and Device Control Policy

- 1 In the console, click **Policies**.
- 2 Under View Policies, click **Application and Device Control**.
- 3 Click the policy that contains the rule set that you want to disable.
- 4 Under Tasks, click **Edit the Policy**.
- 5 Click **Application Control**.
- 6 Uncheck the check box next to the rule set that you want to disable.
- 7 Click **OK**.

You have now disabled a single rule set without disabling the entire policy.

### To disable an individual rule in an Application and Device Control Policy

- 1 In the console, click **Policies**.
- 2 Under View Policies, click **Application and Device Control**.
- 3 Click the policy that contains the rule that you want to disable.
- 4 Under Tasks, click **Edit the Policy**.
- 5 Click **Application Control**.
- 6 Click the rule set that contains the rule that you want to disable, and then click **Edit**.
- 7 Under Rules, in the list of rules, click the rule that you want to disable.
- 8 On the Properties tab, uncheck **Enable this rule**.



- 9 In the Edit Application Control Rule Set dialog box, click **OK**.
- 10 Click **OK**.

You have now disabled a single subordinated rule without disabling the entire policy or rule set.

## Changing the mode of an application control rule set

When you first create an application control rule set, you create it in Test mode. After you test the rule set within a policy, then you can change the mode to Production mode.

### To change the mode of an application control rule set

- 1 In the console, click **Policies**.
- 2 Under View Policies, click **Application and Device Control**.
- 3 Click the policy that contains the application control rule set that you want to change.
- 4 Click **Edit the Policy**.
- 5 Click **Application Control**.
- 6 Click the rule set that you want to change.
- 7 Under Test/Production, click the corresponding drop-down list arrow to display the list of modes.
- 8 Click the new mode.
- 9 Click **OK**.

## Configuring device control for an Application and Device Control Policy

Use device control to manage hardware devices. You can modify this list at any time.

See [“About hardware devices”](#) on page 515.

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

- 1 In the Application and Device Control Policy pane, click **Device Control**.
- 2 Under Blocked Devices, click **Add**.
- 3 Review the list of hardware devices, and click any device or devices that you want to block from accessing the client computer.

- 4 Click **OK**.
- 5 Under Devices Excluded From Blocking, click **Add**.
- 6 Review the list of hardware devices, and click any devices that you want to exclude from being blocked when they access the client computer.
- 7 If you do not want device control information to be logged, uncheck **Log blocked devices**.

The information is logged by default.

- 8 If you want users to be notified, check **Notify users when devices are blocked**.  
If you enabled notification, click **Specify Message Text**, and then type the text that you want the users to see.
- 9 Click **OK**.

# Setting up hardware devices

This chapter includes the following topics:

- [About hardware devices](#)
- [Obtaining a device ID from Control Panel](#)
- [Adding a hardware device](#)
- [Editing a hardware device](#)
- [Deleting a hardware device](#)

## About hardware devices

Use the default list of hardware devices to add a device to an Application and Device Control Policy. The Hardware Devices list eliminates the need to retype these devices each time you want to add one from a rule.

Two numeric values identify devices: device IDs and class IDs. You can use either of these two values to identify devices on the Hardware Devices list.

The Symantec Endpoint Protection Manager console includes lists of the devices that can be blocked and the devices that can be excluded from blocking, as needed. An administrator can add devices, delete devices, or edit the devices in the list.

---

**Note:** You can neither edit nor delete the default devices.

---

## About class IDs

The class ID refers to the Windows GUID. Each device type has both a Class and a ClassGuid associated with it. The ClassGuid is a hexadecimal value with the following format:

```
{00000000-0000-0000-0000-000000000000}
```

## Obtaining a device ID from Control Panel

A device ID is the most specific ID for a device. Devices can have either a specific device ID or a more generic ID. For example, you can specify all USB devices that use one device ID or you can choose one specific removable USB disk drive. You must use the device IDs for the devices that you want to add. You can use either the Symantec DevViewer tool or you can use the Windows Device Manager to get the device IDs. The following is a sample device ID:

```
{IDE\CDROMHL-DT-ST_RW/DVD_GCC-4242N_____0201___\5&3CCF215&0&0.0.0}
```

You do not have to type the entire string. You can use wildcard characters to search for device IDs. For example, you can use the following string in a search:

```
*IDE\CDROM*.
```

### To obtain a device ID from Control Panel

- 1 On the Windows taskbar, click **Start > Settings > Control Panel > System**.
- 2 On the Hardware tab, click **Device Manager**.
- 3 In the Device Manager list, double-click the device.
- 4 In the device's Properties dialog box, on the Details tab, select the Device ID.  
By default, the Device ID is the first value displayed.
- 5 Press **Control+C** to copy the ID string.
- 6 Click **OK** or **Cancel**.

See [“Adding a hardware device”](#) on page 516.

## Adding a hardware device

Devices are listed when you select Hardware Devices on the Policies tab. This list can be used when you develop the access protection policies that involve device-level access control.

### To add hardware devices to the list

- 1 On the Symantec Endpoint Protection Manager console, click **Policies**.
- 2 Under Policy Components, click **Hardware Devices**.
- 3 Under Tasks, click **Add a Hardware Device**.
- 4 Enter the name of the device you want to add and either its Class ID or its Device ID.

Both Class IDs and Device IDs are enclosed in curly braces by convention.

- 5 Click **OK**.

The new device is displayed in the Device Name list. You can also add a device by right-clicking on the hardware devices list on the right, and clicking **Add**.

## Editing a hardware device

You can edit any hardware devices that you have added to the list. The default devices that are listed cannot be edited.

### To edit a hardware device

- 1 On the Symantec Endpoint Protection Manager console, click **Policies**.
- 2 Under Policy Components, click **Hardware Devices**.
- 3 In the Hardware Devices list, click the hardware device you want to edit.
- 4 Click **Edit the Hardware Device**.
- 5 Edit either the device name, the class ID, or the device ID.
- 6 Click **OK**.

The updated device information is displayed in the Identification list.

## Deleting a hardware device

You can delete any of the hardware devices that you have added to the list. The default devices that are listed cannot be deleted.

### To delete a hardware device

- 1 On the Symantec Endpoint Protection Manager console, click **Policies**.
- 2 Under Policy Components, click **Hardware Devices**.
- 3 In the Hardware Devices list, click the hardware device you want to delete.

- 4** Click **Delete the Hardware Device**.
- 5** In the Delete Hardware Device dialog box, click **Yes**.

The hardware device is removed from the Hardware Devices list.

# Customizing Application and Device Control Policies

This chapter includes the following topics:

- [About authorizing the use of applications, patches, and utilities](#)
- [Creating and importing a file fingerprint list](#)
- [About system lockdown](#)
- [Setting up system lockdown](#)

## About authorizing the use of applications, patches, and utilities

Symantec Endpoint Protection Manager gives you the ability to protect client computers from attacks by unapproved applications. It gives you the ability in two ways. First it lets you use file fingerprints to identify approved applications, patches, and the utilities that can run on the client computers. You then decide the action to take when unapproved applications try to access the client computers. If you enable system lockdown, you can then configure Symantec Endpoint Protection Manager to either only log unapproved applications or to use system lockdown to protect those client computers that come under attack by unauthorized programs.

To use system lockdown, you first create a file fingerprint list for each type of client in your environment. A file fingerprint list is a list of approved applications for that client computer. Then you add each of these file fingerprints to a file fingerprint list on the Symantec Endpoint Protection Manager. Lastly, you configure the action to take on the client when an unapproved application tries to access that computer.

For example, create a file fingerprint list for each type of client in your environment. Assume that your environment contains Windows Vista 32-bit, Windows Vista 64-bit, and Windows XP SP2 clients. Run the file, `Checksum.exe`, on an image of each of these three client types that exist in your environment. `Checksum.exe` generates file fingerprints for all of the applications for each client type and puts them into a file fingerprint list. In this example, you end up with three file fingerprint lists: one for each image.

Next, use Symantec Endpoint Protection to create a file fingerprint list to which you add each of the three file fingerprint lists you generated: one file fingerprint list for each client type. Then, you define what action Symantec Endpoint Protection takes when an unapproved application tries to access a client computer. You can disable system lockdown and allow application access. You can choose to only log the unapproved applications. For the most protection, you can enable system lockdown on the client computer that the unauthorized application is trying to access.

## Creating and importing a file fingerprint list

A file fingerprint list for a client computer image consists of a list of checksums for each application on that client computer along with the complete file paths of those applications. You can verify that each image contains all of the executables that are approved for use at your company. To create a file fingerprint list, you can use the utility `Checksum.exe` that is installed along with Symantec Endpoint Protection on the client computer. You can run this command on each computer image in your environment to create a file fingerprint list for those images. The file `Checksum.exe` is located in the following location:

`C:\Program Files\Symantec\Symantec Endpoint Protection`

You can run this tool from the command prompt. `Checksum.exe` creates a text file that contains a list of all executables on that computer and their corresponding checksums.

You can use Symantec Endpoint Protection Manager to import file fingerprint lists for each client computer type into a master file fingerprint list. You can manage the file fingerprint list using Symantec Endpoint Protection Manager. The file fingerprint list contains the approved files for all of your client computers. You can also add file fingerprints for individual files you want to approve.

### Creating a file fingerprint list

You can use `Checksum.exe` to create a file fingerprint list. The file fingerprint list names each file and corresponding checksum that resides on the client computer image. This tool is provided with Symantec Endpoint Protection on the client.



### To create a file fingerprint list

- 1 Go to the computer that contains the image for which you want to create a file fingerprint list. The computer must have Symantec Endpoint Protection client software installed.
- 2 Open a command prompt window.
- 3 Navigate to the directory that contains the file `Checksum.exe`. By default, this file is located in the following location:

C:\Program Files\Symantec\Symantec Endpoint Protection

- 4 Type the following command:

```
checksum.exe outputfile drive
```

where *outputfile* is the name of the text file that contains the checksums for all the executables that are located on the specified drive. The output file is a text file (*outputfile.txt*).

The following is an example of the syntax you use:

```
checksum.exe cdrive.txt c:\
```

This command creates a file that is called `cdrive.txt`. It contains the checksums and file paths of all the executables and DLLs found on the C drive of the client computer on which it was run.

### Sample Checksum.exe output

A sample of a `Checksum.exe` output file that was run on a computer image follows. The format of each line is *checksum\_of\_the\_file* space *full\_pathname\_of\_the\_exe\_or\_DLL*.

```
0bb018fad1b244b6020a40d7c4eb58b7 c:\dell\openmanage\remind.exe  
35162d98c2b445199fef95e838feae4b c:\dell\pnp\m\co\HSFCI008.dll  
77e4ff0b73bc0aeaf39bf0c8104231f c:\dell\pnp\m\co\HSFHWBS2.sys  
f59ed5a43b988a18ef582bb07b2327a7 c:\dell\pnp\m\co\HSF_CNXT.sys  
60e1604729a15ef4a3b05f298427b3b1 c:\dell\pnp\m\co\HSF_DP.sys  
4f3ef8d2183f927300ac864d63dd1532 c:\dell\pnp\m\co\HXFSetup.exe  
dcd15d648779f59808b50f1a9cc3698d c:\dell\pnp\m\co\MdmXSdk.dll  
eeaea6514ba7c9d273b5e87c4e1aab30 c:\dell\pnp\m\co\MDMXSDK.sys  
0a7782b5f8bf65d12e50f506cad6d840 c:\dell\pnp\mgmt\drac2wdm.sys  
9a6d7bb226861f6e9b151d22b977750d c:\dell\pnp\mgmt\racser.sys  
d97e4c330e3c940ee42f6a95aec41147 c:\dell\pnp\n\bc\b57xp32.sys
```

## Editing a file fingerprint list

You cannot directly edit an existing file fingerprint list. First, you can use Checksum.exe to create a new file fingerprint list by using a different computer image. You can then merge the existing file fingerprint list on the Symantec Endpoint Protection Manager with the new file fingerprint list from a client image.

### To edit a file fingerprint list

- 1 In the Symantec Endpoint Protection Manager console, click **Policies**.
- 2 Under View Policies, expand **Policy Components**, and then click **File Fingerprint List**.
- 3 In the File Fingerprint Lists pane, right-click the fingerprint list that you want to edit.
- 4 Click **Edit**.
- 5 In the Edit File Fingerprint Wizard, click **Next**.
- 6 Click **Append a fingerprint file to this file fingerprint** to add a new file to the existing one, and then click **Next**.
- 7 Click **Browse** to locate the file or type the full path of the file fingerprint list in the text box.
- 8 Click **Next**.
- 9 Click **Close**.
- 10 Click **Finish**.

## Importing a file fingerprint list into a shared policy

You can add file fingerprint lists to a shared policy by importing a file. You must have created the list already.

See [“Creating a file fingerprint list”](#) on page 520.

### To import a file fingerprint list into a shared policy

- 1 In the Symantec Endpoint Protection Manager console, click **Policies**
- 2 Under View Policies, expand **Policy Components**, and then click **File Fingerprint List**.
- 3 Under Tasks, click **Add a File Fingerprint List**.
- 4 In the Welcome to the Add File Fingerprint Wizard pane, click **Next**.
- 5 In the Information about New File Fingerprint panel, in the Name text box, type the name of the fingerprint list that you want to add.

- 6 In the Information about New File Fingerprint panel, in the Description text box, type a description of the fingerprint list that you want to add.  
This step is optional.
- 7 Click **Next**.
- 8 In the Create a File Fingerprint panel, click **Create the file fingerprint by importing a file fingerprint file**.
- 9 Click **Next**.
- 10 Click **Browse** to locate the file, or type the full path of the file fingerprint list in the text box.
- 11 Click **Next**.
- 12 Click **Close**.
- 13 Click **Finish**.

The new list appears in the File Fingerprint Lists on the right.

## Merging file fingerprint lists into a shared policy

You can merge multiple file fingerprint lists that exist in a shared policy. You must have already added the lists that you want to merge before you start this task.

See [“Importing a file fingerprint list into a shared policy”](#) on page 522.

### To merge file fingerprint lists into a shared policy

- 1 In the Symantec Endpoint Protection Manager console, click **Policies**.
- 2 Under View Policies, expand **Policy Components**, and then click **File Fingerprint List**.
- 3 In the Welcome to the Add File Fingerprint Wizard pane, click **Next**.
- 4 In the Information about New File Fingerprint panel, in the Name text box, type the name of the merged fingerprint list that you want to add.
- 5 In the Information about New File Fingerprint panel, in the Description text box, type a description of the merged fingerprint list that you want to add.  
This step is optional.
- 6 Click **Next**.
- 7 In the Create a File Fingerprint panel, click **Create the file fingerprint by combining multiple existing file fingerprints**.

This option is only available if you have existing file fingerprint lists in a shared policy.

- 8 Click **Next**.
- 9 Select the fingerprint lists that you want to merge.
- 10 Click **Next**.
- 11 Click **Close**.
- 12 Click **Finish**.

The merged fingerprint list appears in the File Fingerprint Lists on the right.

## Deleting a file fingerprint list

You can delete any file fingerprint lists that you no longer need. First make sure that the file fingerprint list is no longer needed at the group level before you delete it from a shared policy.

### To delete a file fingerprint list

- 1 In the Symantec Endpoint Protection Manager console, click **Policies**.
- 2 Under View Policies, expand **Policy Components**, and then click **File Fingerprint List**.
- 3 In the File Fingerprint Lists pane, click the file fingerprint list that you want to delete.
- 4 Under Tasks, click **Delete the List**.
- 5 Click **Yes** to confirm.

The file fingerprint list is deleted from the Symantec Endpoint Protection Manager, but it remains on the computer in the location from which you imported it.

## About system lockdown

System lockdown is a protection setting that you can use to control the applications that can run on the client computer. You can create a file fingerprint list that contains the checksums and the locations of all the applications that are authorized for use at your company. The client software includes a Checksum.exe tool that you can use to create a file fingerprint list. The advantage of system lockdown is that it can be enforced whether or not the user is connected to the network.

You can use system lockdown to block almost any Trojan horse, spyware, or malware that tries to run or load itself into an existing application. For example, you can prevent these files from loading into Internet Explorer. System lockdown ensures that your system stays in a known and trusted state.

Applications that run on the client computer can include the following executable files:

- .exe
- .com
- .dll
- .ocx

Symantec recommends that you implement system lockdown in the following stages:

Get an approved software image	Create a software image that includes all of the applications you want users to be able to use on their computers. Use this image to create a file fingerprint list.
Log unapproved applications	Enable system lockdown by logging the applications that are not included in the file fingerprint list. You can then adjust your file fingerprint to include the required applications of users. You can give them appropriate warning before blocking unapproved applications.
Add allowed applications	Add the executables that you want to be allowed even if they are not in the file fingerprint list.
Enable system lockdown	Enforce system lockdown and block unapproved applications.

You have the option to define a custom message to display to users who have blocked applications.

## System lockdown prerequisites

The following prerequisites must be met before you can enable system lockdown:

Create file fingerprint list	You need to have created a file fingerprint list that includes the applications that are allowed. This list can be created from a corporate image that is installed regularly on users' computers. You create this list on a computer that runs the client.
Add one or more file fingerprint lists	After you create the fingerprint lists, you need to add them to the manager.

Merge file fingerprint lists

Multiple file fingerprint lists can be merged. For example, you may use different images for different groups at your company.

You implement system lockdown in the following stages:

Set up and test system lockdown

Before you block unapproved executables, you can add one or more file fingerprint lists. Add the applications that should always be allowed, and log the results in the Control log.

Check the unapproved applications list

After a few days of testing system lockdown, you can view the list of unapproved applications. This list shows the unapproved applications that users in the group run. You can decide whether to add more applications to the file fingerprint or to the allowed list.

Enable system lockdown

Next, you can enable system lockdown blocking the applications that are not included in the file fingerprint lists.

## Setting up system lockdown

To set up system lockdown, you follow a two-step process:

- In step 1, you monitor the applications that the client computers run. In this step, you can track these applications in a list of unapproved applications. The list of unapproved applications includes the applications that clients run but are not listed in the file fingerprint list of approved applications. The client does not block the unapproved applications. You can track the applications that clients use for informational purposes before you block those applications. You can also test whether any applications appear on the unapproved applications list. If a test runs, the status says how long it has been running and whether or not exceptions have occurred. Run system lockdown in test mode long enough to discover which unapproved applications the client computers run. Then enable system lockdown.
- In step 2, you enable system lockdown. After you run system lockdown in test mode long enough to see which unapproved applications are run, you enable the following settings:

Approve the use of those additional applications	Add applications to the list of approved applications, or add the applications to the image where you created the file fingerprint.
Notify users	You can notify a user that the user no longer has access to a computer. You can also inform the user that the specified applications can be used at some future date that you state. You then proceed to enable system lockdown on that date.
Continue to log the use of the unapproved applications	No further action is necessary.

---

**Note:** You can also create firewall rules to allow approved applications on the client.

---

### To set up system lockdown

- 1 On the console, click **Clients**.
- 2 Under View Clients, locate the group for which you want to set up system lockdown.
- 3 On the Policies tab, click **System Lockdown**.
- 4 In the System Lockdown for *name of group* dialog box, click **Step 1: Log Unapproved Applications Only** if you want to turn on this protection in test mode.  
  
This option logs the unapproved network applications that clients are currently running.
- 5 Click **Step 2: Enable System Lockdown** if you want to turn on this protection. This step blocks the unapproved applications that clients try to run.
- 6 Under Approved Applications, select the file fingerprint list to use as the approved executables list.  
  
See [“Editing a file fingerprint list”](#) on page 522.
- 7 If you want to add additional file fingerprint lists, click **Add**, click the list name, and then click **OK** to add additional file fingerprint lists.
- 8 Check **Test Before Removal** for the applications that you want to test before the client blocks the applications.

- 9 To view the list of unapproved applications, click **View Unapproved Applications**.

In the Unapproved Applications dialog box, review the applications. This list includes information about the time that the application was run, the computer host name, the client user name, and the executable file name.

- 10 Determine how you want to handle the unapproved applications.

You can add the names of applications that you want to allow to the list of approved applications. You can add the executable to the computer image the next time that you create a file fingerprint.

- 11 Click **Close**.

- 12 To specify the executables that are always allowed even if they are not included in the file fingerprint list, under the File Name list, click **Add**.

- 13 In the Add File Definition dialog box, specify the full path name of the executable file (.exe or .dll).

Names can be specified using a normal string or regular expression syntax. Names can include wildcard characters (\* for any characters and ? for one character). The name can also include environment variables such as %ProgramFiles% to represent the location of your Program Files directory or %windir% for the Windows installation directory.

- 14 Either leave **Use wildcard matching (\* and ? supported)** selected by default, or click **Use regular expression matching** if you used regular expressions in the filename instead.

- 15 If you want to allow the file only when it is executed on a particular drive type, click **Only match files on the following drive types**.

Then unselect the drive types you do not want to include. By default, all drive types are selected.

- 16 If you want to match by device id type, check **Only match files on the following device id type**, and then click **Select**.

- 17 Click the device you want in the list, and then click **OK**.

- 18 Click **OK**.

- 19 To display a message on the client computer when the client blocks an application, check **Notify the user if an application is blocked**.

- 20 To write a custom message, click **Notification**, type the message, and click **OK**.

- 21 Click **OK**.



# Configuring centralized exceptions

- [Configuring Centralized Exceptions Policies](#)



# Configuring Centralized Exceptions Policies

This chapter includes the following topics:

- [About Centralized Exceptions Policies](#)
- [Configuring a Centralized Exceptions Policy](#)
- [Configuring client restrictions for centralized exceptions](#)
- [Creating centralized exceptions from log events](#)

## About Centralized Exceptions Policies

Centralized Exceptions Policies contain exceptions for the following types of scans:

- Antivirus and antispyware scans
- TruScan proactive threat scans
- Tamper Protection scans

---

**Note:** Antivirus and antispyware scans include all Auto-Protect scans, scheduled scans, on-demand scans, or user-defined scans.

---

Typically, exceptions are risks or processes that you want the client software to exclude from scans. If you use exceptions on client computers, you might reduce the scan time. If you reduce the scan time, you increase system performance on the client computers.

For TruScan proactive threat scans, you might also want the client software to detect a specific process that it does not detect by default. You can create an

exception to force the detection. When the detection appears in the detected processes list, you can create another exception to specify an action for the detection.

---

**Note:** For antivirus and antispyware scans or Tamper Protection, you use centralized exceptions to specify particular items to exclude from scans. For proactive threat scans, however, you use centralized exceptions to specify actions for detected processes or to force a detection.

---

When you create a Centralized Exceptions Policy, the exceptions apply to all scans of that type on the client computer that uses the policy. You can include all of the exceptions in the same policy.

Unlike other policies, the Symantec Endpoint Protection Manager console does not include a default Centralized Exceptions Policy. You must create a new policy. You can create Centralized Exceptions Policies from the Policies page, or you can create Centralized Exceptions Policies from the Clients page in the management console.

You can add exceptions to a Centralized Exceptions Policy by using the logs in the management console. You must create a Centralized Exceptions Policy before you can use this method to create exceptions.

See [“Creating centralized exceptions from log events”](#) on page 540.

## About working with Centralized Exceptions Policies

You create and edit Centralized Exceptions Policies similarly to how you create and modify other types of policies. You can assign, withdraw, replace, copy, export, import, or delete a Centralized Exceptions Policy.

You typically assign a policy to multiple groups in your security network. You can create a non-shared, location-specific policy if you have specific requirements for a particular location.

To work with Centralized Exceptions Policies, you must be familiar with the basics of policy configuration.

See [“About working with policies”](#) on page 322.

## About centralized exceptions for antivirus and antispyware scans

You may want to exclude a particular security risk from antivirus and antispyware scans. You might want to exclude particular files, folders, or file extensions from the scans.

When you exclude a security risk, scans ignore the risk. You can configure the exception so that the scans log the detection. In either case, the client software does not notify users when it detects the specified security risks. When you exclude files, folders, or extensions, the scans ignore the files, folders, or extensions.

---

**Note:** Centralized exceptions apply to all antivirus and antispyware scans. You cannot create different exceptions for different types of scans. For example, you may want to create a centralized exception to exclude a particular file extension. The client software then excludes the extension from Auto-Protect scans and all administrator-defined scans and user-defined scans. Administrator-defined scans and user-defined scans include scheduled scans and on-demand scans.

---

## About centralized exceptions for TruScan proactive threat scans

You may want to exclude certain processes from proactive threat scans. You need to determine that the processes that you want to exclude are safe to run on the client computers in your security network. To exclude a detected process, you set the detection action to Ignore.

You can also create a centralized exception to specify that certain processes are not permitted. To specify that processes are not permitted, you set the detection action to Quarantine or Terminate.

You can force a proactive threat detection by creating a centralized exception that specifies a file name. When the proactive threat scan detects the file, the client logs the instance. Because file names are not unique, multiple processes might use the same file name. You can use a forced detection to help you create an exception to quarantine or terminate a process that is associated with the file.

See [“How TruScan proactive threat scans work with centralized exceptions”](#) on page 488.

## About centralized exceptions for Tamper Protection

Tamper Protection protects client computers from the processes that tamper with Symantec processes and internal objects. When Tamper Protection detects a process that might modify the Symantec configuration settings or Windows registry values, it blocks the process. You might need to allow an application to modify Symantec settings. You might want to stop Tamper Protection for certain areas of the registry or certain files on the client computer.

In some cases, Tamper Protection might block a screen reader or some other assistive technology application. You can create a centralized exception so that the application can run on client computers.

## About client interaction with centralized exceptions

Administrator-defined exceptions always take precedence over user-defined exceptions. On client computers, users can view the list of administrator-defined exceptions but cannot change them. A user can also view any exception that the user creates.

By default, users on client computers have limited configuration rights for centralized exceptions.

By default, users have the following restrictions:

- Users cannot create exceptions to force detections for proactive threat scans. Users cannot select from a list of detected processes to create an exception for proactive threat scans. However, users can select a file on the client computer to create a proactive threat scan exception.
- Users cannot create any exceptions for Tamper Protection.

You can restrict users on client computers so that they cannot create exceptions for antivirus and antispysware scans or for proactive threat scans.

See [“Configuring client restrictions for centralized exceptions”](#) on page 540.

## Configuring a Centralized Exceptions Policy

You configure a Centralized Exceptions Policy similarly to how you configure other types of policies.

You can click Help for more information about the options that are used in the procedures.

### To configure a Centralized Exceptions Policy

- 1 On the Centralized Exceptions Policy page, click **Centralized Exceptions**.
- 2 Under Centralized Exceptions, click **Add**, and then do any of the following actions:
  - Click **Security Risk Exceptions**, and then add a security risk exception that you want to include in the policy.  
See [“Configuring a centralized exception for antivirus and antispysware scans”](#) on page 535.
  - Click **TruScan Proactive Threat Scan Exceptions**, and then add a proactive threat scan exception that you want to include in the policy.  
See [“Configuring a centralized exception for TruScan proactive threat scans”](#) on page 537.

- Click **Tamper Protection Exception**, and then add a Tamper Protection scan exception that you want to include in the policy.  
See “[Configuring a centralized exception for Tamper Protection](#)” on page 539.
- 3 Repeat step 2 to add more exceptions.
  - 4 If you are finished with the configuration for this policy, click **OK**.

## Configuring a centralized exception for antivirus and antispyware scans

You can create exceptions for known security risks, files, folders, or file extensions. The exceptions apply to all antivirus and antispyware scans that run on the client computers that use the policy.

You can click Help for more information about the options that are used in the procedure.

### To configure a centralized exception for antivirus and antispyware scans

- 1 On the Centralized Exceptions Policy page, click **Centralized Exceptions**.
- 2 Under Centralized Exceptions, click **Add > Security Risk Exceptions**, and then do one of the following actions:
  - Click **Known Risks**, and then configure the exception.  
See “[Configuring centralized exceptions for known security risks](#)” on page 535.
  - Click **File**, and then configure the exception.  
See “[Configuring a centralized exception for a file](#)” on page 536.
  - Click **Folder**, and then configure the exception.  
See “[Configuring a centralized exception for a folder](#)” on page 536.
  - Click **Extensions**, and then configure the exception.  
See “[Configuring a centralized exception for a file extension](#)” on page 537.
- 3 Click **OK**.
- 4 If you are finished with the configuration for this policy, click **OK**.

### Configuring centralized exceptions for known security risks

The security risks that the client software detects appear in the Known Security Risk Exceptions dialog box.

The known security risks list includes information about the severity of the risk.

You can click Help for more information about the centralized exceptions options for known security risks.

### To configure centralized exceptions for known security risks

- 1 On the Centralized Exceptions Policy page, click **Centralized Exceptions**.
- 2 Under Centralized Exceptions, click **Add > Security Risk Exceptions > Known Risks**.
- 3 In the Known Security Risk Exceptions dialog box, select one or more security risks that you want to exclude from antivirus and antispyware scans.
- 4 Check **Log when the security risk is detected** if you want to log the detection.  
If you do not check this option, the client ignores the risk when it detects the selected risks. The client therefore does not log the detection.
- 5 Click **OK**.
- 6 If you are finished with the configuration for this policy, click **OK**.

### Configuring a centralized exception for a file

You add exceptions for files individually. If you want to create exceptions for more than one file, repeat the procedure.

#### To configure a centralized exception for a file

- 1 On the Centralized Exceptions Policy page, click **Centralized Exceptions**.
- 2 Under Centralized Exceptions, click **Add > Security Risk Exceptions > File**.
- 3 Under Security Risk File Exception, in the Prefix variable drop-down box, select a file location if you want to restrict the exception.  
Click **NONE** if you want the exception to apply to the file in any location on the client computer.
- 4 In the File text box, type the name of the file.  
Include any path information for the file.
- 5 Click **OK**.
- 6 If you are finished with the configuration for this policy, click **OK**.

### Configuring a centralized exception for a folder

You add exceptions for folders individually. If you want to create exceptions for more than one folder, repeat the procedure.

#### To configure a centralized exception for a folder

- 1 On the Centralized Exceptions Policy page, click **Centralized Exceptions**.
- 2 Under Centralized Exceptions, click **Add > Security Risk Exceptions > Folder**.



- 3 Under Security Risk Folder Exception, in the Prefix variable drop-down box, select a folder location if you want to restrict the exception.  
Click **NONE** if you want the exception to apply to the file in any location on the client computer.
- 4 In the Folder text box, type the name of the folder.  
Include any path information for the folder.
- 5 Click **OK**.
- 6 If you are finished with the configuration for this policy, click **OK**.

### Configuring a centralized exception for a file extension

You can add multiple file extensions to an exception. After you create the exception, you cannot create another extensions exception for the same policy. You must edit the existing exception.

---

**Note:** You can add only one extension at a time. If you enter multiple extension names in the Add text box, the policy treats the entry as a single extension name.

---

#### To configure a centralized exception for a file extension

- 1 On the Centralized Exceptions Policy page, click **Centralized Exceptions**.
- 2 Under Centralized Exceptions, click **Add > Security Risk Exceptions > Extension**.
- 3 In the text box, type the extension that you want to exclude, and then click **Add**.
- 4 Repeat step 3 to add more extensions to the exception.
- 5 Click **OK**.
- 6 If you are finished with the configuration for this policy, click **OK**.

## Configuring a centralized exception for TruScan proactive threat scans

You can configure exceptions to exclude detected processes from future proactive threat scans. You can also force a proactive threat scan to detect a particular process.

#### To configure a centralized exception for TruScan proactive threat scans

- 1 On the Centralized Exceptions Policy page, click **Centralized Exceptions**.
- 2 Click **Add > TruScan Proactive Threat Scan Exceptions**, and then do one of the following actions:

- Click **Detected Processes**.  
See [“Configuring a centralized exception for a detected process”](#) on page 538.
  - Click **Process**.  
See [“Configuring an exception to force TruScan proactive threat scans to detect a process”](#) on page 538.
- 3 Click **OK**.
  - 4 If you are finished with the configuration for this policy, click **OK**.

## Configuring a centralized exception for a detected process

You can create an exception for a process that TruScan proactive threat scans detect.

When you create an exception for a detected process, you choose from a list of detections. The management console populates the list with the detections that the client logs in your security network.

The detection list appears empty if the client computers in your network have not yet made any detections.

You can force proactive threat scans to detect a particular process. When a proactive threat scan detects the process, and the management console receives the event, the process appears in the detected process list.

See [“Configuring an exception to force TruScan proactive threat scans to detect a process”](#) on page 538.

### To configure a centralized exception for a detected process

- 1 On the Centralized Exceptions Policy page, click **Centralized Exceptions**.
- 2 Click **Add > TruScan Proactive Threat Scan Exceptions > Detected Processes**.
- 3 Select the processes for which you want to create an exception.
- 4 In the Action drop-down box, select **Ignore**, **Terminate**, **Quarantine**, or **Log only**.
- 5 Click **OK**.
- 6 If you are finished with the configuration for this policy, click **OK**.

## Configuring an exception to force TruScan proactive threat scans to detect a process

You can configure an exception to force proactive threat scans to detect a process. You might configure this type of exception when proactive threat scans currently do not detect a particular process.

After future scans run and detect the specified process, you can create another exception to handle the process.

See “[Configuring a centralized exception for a detected process](#)” on page 538.

#### To configure an exception to force TruScan proactive threat scans to detect a process

- 1 On the Centralized Exceptions Policy page, click **Centralized Exceptions**.
- 2 Click **Add > TruScan Proactive Threat Scan Exceptions > Process**.
- 3 In the dialog box, type the process name.  
For example, you might type the name of an executable file as follows:  
**foo.exe**
- 4 Click **OK**.
- 5 If you are finished with the configuration for this policy, click **OK**.

## Configuring a centralized exception for Tamper Protection

You can configure centralized exceptions for Tamper Protection. You need to know the file name that is associated with the application that you want to allow.

For example, Tamper Protection might block an assistive technology application, such as a screen reader. You need to know the name of the file associated with the assistive technology application. Then you can create an exception to allow the application to run.

#### To configure a centralized exception for Tamper Protection

- 1 On the Centralized Exceptions Policy page, click **Centralized Exceptions**.
- 2 Click **Add > Tamper Protection Exception**.
- 3 In the Tamper Protection Exception dialog box, in the Prefix variable drop-down box, select a file location if you want to restrict the exception.
- 4 In the File text box, type the name of the file.  
Include any path information for the file.
- 5 Click **OK**.
- 6 If you are finished with the configuration for this policy, click **OK**.

## Configuring client restrictions for centralized exceptions

You can configure restrictions so that users on client computers cannot create exceptions for antivirus and antispyware scans or for TruScan proactive threat scans. By default, users are permitted to configure exceptions. For proactive threat scans, users have limited configuration privileges.

You can click Help for more information about the options that are used in the procedure.

---

**Note:** Users on client computers can never create exceptions for Tamper Protection, regardless of the restriction settings.

---

### To configure client restrictions for centralized exceptions

- 1 On the Centralized Exceptions Policy page, click **Client Restrictions**.
- 2 Under Client Restrictions, check or uncheck **Security risk exceptions** and **TruScan proactive threat scan exceptions**.
- 3 If you are finished with the configuration for this policy, click **OK**.

## Creating centralized exceptions from log events

You can create centralized exceptions from log events for antivirus and antispyware scans or proactive threat scans. You cannot create exceptions from log events for Tamper Protection.

When you create exceptions from log events, you add a risk, file, folder, extension, or process to the centralized exceptions policy. You specify the Centralized Exceptions Policy when you create the exception.

See [“About logs”](#) on page 171.

### To create centralized exceptions from log events

- 1 On the Monitors tab, click the **Logs** tab.
- 2 In the Log type drop-down list, select one of the following options:
  - **Risk**
  - **TruScan Proactive Threat Scan**
  - **Application and Device Control**

- 3 If you selected Application and Device Control, select **Application Control** from the Log content list.
- 4 Click **View Log**.
- 5 Follow the instructions for adding centralized exceptions for the type of log that you selected.  
 See [“Adding a centralized exception for risk events”](#) on page 541.  
 See [“Adding a centralized exception for TruScan proactive threat scan events”](#) on page 541.  
 See [“Adding a centralized exception for Tamper Protection events”](#) on page 542.

## Adding a centralized exception for risk events

You can add a centralized exception for risk events.

### To add a centralized exception for risk events

- 1 On the Risk Logs page, select one or more events for which you want to add a centralized exception.
- 2 Next to Action, select one of the following options:
  - **Add Risk to Centralized Exceptions Policy**
  - **Add File to Centralized Exceptions Policy**
  - **Add Folder to Centralized Exceptions Policy**
  - **Add Extension to Centralized Exceptions Policy**
- 3 Click **Start**.
- 4 In the dialog box, you can remove any of the risks, files, folders, or extensions that are associated with the event. If you remove items, you do not include them in the exception.  
 If no items appear in the risks, files, folders, or extensions list, you cannot create an exception.
- 5 For security risks, check **Log when the security risk is detected** if you want the client software to log the detection.
- 6 Select all of the centralized exceptions policies that should use this exception.
- 7 Click **OK**.

## Adding a centralized exception for TruScan proactive threat scan events

You can add a centralized exception for proactive threat scan events.

#### To add a centralized exception for TruScan proactive threat scan events

- 1 On the TruScan Proactive Threat Scan Logs page, select one or more events for which you want to add a centralized exception.
- 2 Next to Action, select **Add Process to Centralized Exceptions Policy**.
- 3 Click **Start**.
- 4 In the dialog box, in the Response drop-down list, select the detection action for the process.  
  
Optionally, you can remove any processes that you do not want to include in the exception.
- 5 Select the Centralized Exceptions Policies that should include this exception.
- 6 Click **OK**.

## Adding a centralized exception for Tamper Protection events

You can add a centralized exception for Tamper Protection events. The Tamper Protection feature must have already blocked the application that you want to allow. After Tamper Protection blocks the application, the client computer logs the event and sends it to the management server. You can use the log event to create the exception.

#### To add a centralized exception for Tamper Protection events

- 1 On the Application and Device Control Logs page, select one or more events for which you want to add a centralized exception.  
  
For example, you might select one or more events that apply to the assistive technology applications that you want to run.
- 2 Next to Action, select **Add File to Centralized Exceptions Policy**.
- 3 Click **Start**.
- 4 To remove a file that you do not want to include in the exception, select the file and click **Remove**.  
  
Repeat this step to remove more files.
- 5 Select the Centralized Exceptions Policies that should include this exception.
- 6 Click **OK**.

# Configuring Host Integrity for endpoint policy compliance

- [Basic Host Integrity settings](#)
- [Adding custom requirements](#)





# Basic Host Integrity settings

This chapter includes the following topics:

- [How Host Integrity enforcement works](#)
- [About working with Host Integrity Policies](#)
- [About Host Integrity requirement planning](#)
- [Adding Host Integrity requirements](#)
- [Editing and deleting a Host Integrity requirement](#)
- [Enabling and disabling Host Integrity requirements](#)
- [Changing the sequence of Host Integrity requirements](#)
- [Adding a Host Integrity requirement from a template](#)
- [About settings for Host Integrity checks](#)
- [About Host Integrity remediation](#)
- [Specifying the amount of time the client waits to remediate](#)
- [Allowing users to postpone or cancel Host Integrity remediation](#)

## How Host Integrity enforcement works

You set up Host Integrity Policies to ensure that the client computers that connect to an enterprise network run the required applications and data files. The client that runs a Host Integrity check implements the Host Integrity Policy settings that you set up. The client enforces these policies by taking action on its own, such as downloading a patch or starting a program. You can also use an Enforcer to enforce these policies. The Enforcer is either a software application or an

optional hardware appliance that mediates the connectivity of the client to the network. Most examples that are shown here show the use of an Enforcer.

During the Host Integrity check, the client follows the requirements that are set in the Host Integrity Policy. It examines the registry keys, active applications, date and size of a file, and other possible parameters to determine the existence of the required software.

The client automatically generates an entry in the Security log whenever it finds that the required software is not installed on the computer. If user notification is enabled on the client, a message appears on the user's computer.

If the required software is not installed on the computer, the client can be set to silently connect to a remediation server. From there it can download and install the required software. The software can include a software patch, a hotfix, an update to virus definitions, and so on. The client can give the user a choice to download immediately or postpone a download. The computer cannot connect to the enterprise network until the software is installed.

The client can also detect whether or not an antivirus application is out of date. If an antivirus application is older than what a system administrator has specified, the client can be prevented from connecting to the enterprise network. Before it can connect, the client needs an up-to-date version of the antivirus application.

The Host Integrity Policy includes the settings that determine how often the client runs a Host Integrity check on the client computer. The client computer can connect to the network through a Symantec Enforcer. You can set up the Host Integrity Policy so that the client runs the Host Integrity check only when the Enforcer prompts the client. The Enforcer can verify the following: the client is running, the client's policy is up to date, and the Host Integrity check is passed before it allows access to the network.

Every time a client receives a new security policy, it immediately runs a Host Integrity check. The client can be set up to automatically download and install the latest security policy. A Security log entry is generated if the policy update fails. If user notification is enabled on the client, a message appears on the user's computer.

You can consider some of the following examples when you set up the requirements for Host Integrity enforcement:

- The client runs up-to-date antivirus software.
- The Host Integrity check is done only when the client tries to connect to the network through an Enforcer.
- The check triggers the actions that takes place silently on the client.

The Enforcer automatically does the following actions:

- Verifies that a client has been installed on a user's computer
- Prompts a client to retrieve updated security policies, if available

The Enforcer then prompts the client to run the Host Integrity check.

The client first verifies that the latest antivirus software is installed and runs. If it has been installed but is not running, the client silently starts the antivirus application. If it is not installed, the client downloads the software from a URL that is specified in the Host Integrity requirement. Then the client installs and starts the software.

Next, the client verifies that the antivirus signature files are current. If the antivirus files are not current, the client silently retrieves and installs the updated antivirus files.

The client runs the Host Integrity check again and passes. The Enforcer receives the results and grants the client access to the enterprise network. In this example, the following requirements must be met:

- The file server that is used for Host Integrity updates has the latest files installed. The client obtains updated applications from the file server. You can set up one or more remediation servers that are connected to the enterprise network. From the remediation servers, users can copy or automatically download the required patches and hotfixes for any required application. If a remediation server fails, then Host Integrity remediation also fails. If the client tries to connect through an Enforcer, the Enforcer blocks the client if Host Integrity fails. The console includes a feature to pass the Host Integrity check even though the check fails. In this case, the Enforcer does not block the client. Information about the failed Host Integrity check is recorded in the client's Security log.
- The management server must be configured so that updates of the security policy are automatically sent to any computer that runs the client.

If the parameters that are defined for the Host Integrity Policies are not successful, then the Enforcer blocks the client from connecting to the network. The following message appears on the client:

```
Symantec Enforcer has blocked all traffic from the client.  
rule: {name of requirement} failed.
```

If the Enforcer blocks the client, the client tries to recover. If the Host Integrity Policy is set up to update files before it allows the client to connect to the network, then the user is notified that an update needs to be provided. A progress indicator for the update follows the update. If the user disconnects from the enterprise network, the process starts again.

## About working with Host Integrity Policies

You create and edit Host Integrity Policies similarly to how you create and modify other types of policies. You can assign, withdraw, replace, copy, export, import, or delete a Host Integrity Policy.

You typically assign a policy to multiple groups in your security network. You can create a non-shared, location-specific policy if you have specific requirements for a particular location.

To work with Host Integrity Policies, you must be familiar with the basics of policy configuration.

See [“About working with policies”](#) on page 322.

## About the Quarantine Policy

The Quarantine Policy is a policy for the Symantec Network Access Control client that runs the Host Integrity check. If the Host Integrity Policy requirements are not met, the client tries remediation. If remediation fails, the client automatically switches to a Quarantine Policy. A Quarantine Policy can be an Antivirus and Antispyware Policy, Firewall Policy, Intrusion Prevention Policy, LiveUpdate Policy, or Application and Device Control Policy. You can set up and assign a Quarantine Policy to a location.

## About Host Integrity requirement planning

When you plan Host Integrity requirements, you must consider the following issues:

- What software (applications, files, patches, and so on) do you want to require for enterprise security?
- What occurs if a requirement is not met? For example:
  - The client can connect to a server and restore the software to meet the requirement.
  - The Host Integrity check can pass even though the requirement fails.
  - The Host Integrity check can fail and network access can be blocked.
  - A pop-up message can notify the user what to do next.

Consider the following areas in more detail:

- Which antivirus applications, antispyware applications, firewall applications, patches, or updates are required on every user’s computer when it connects to the network? You usually create a separate requirement for each type of

software. Predefined Host Integrity requirements let you easily set up these commonly used requirements.

- You can give users the right to select which firewall, antispyware, or antivirus applications they want to run on their computers. The predefined requirements let you specify either a specific application or an entire list of supported applications as acceptable. You can create a custom requirement that includes the applications that are acceptable in your company.
- How to handle restoring the user's computer to meet the requirements? Normally, you need to set up a remediation server with the required software. When you configure the requirement, you must specify the URL from which the client can download and install the required software.
- Some patches require a user to restart the computer. Updates are completed in a specific order so that all updates are applied before a user has to restart. As part of the Host Integrity Policy, you can set the order in which requirements are checked and the remediation is tried.
- You should also consider what occurs if a requirement fails and cannot be restored. For each requirement, you have the choice to allow the Host Integrity check to pass even though that requirement fails. As part of the general Host Integrity Policy, you also can configure pop-up messages. The client displays these pop-up messages to the user if the Host Integrity check fails or if it passes after previous failure. You may want to plan additional instructions for the user in these pop-up messages. In addition, you can set up a quarantine policy to activate if Host Integrity fails.
- You can simplify the management of required applications by including similar applications in one custom requirement. For example, you can include Internet browsers such as the Internet Explorer and Netscape Navigator in one requirement.
- As part of a custom requirement, you can specify whether to allow the Host Integrity check to pass if the requirement fails. When you plan how many conditions to check for in one script, remember that this setting applies to the custom requirement script as a whole. This aspect of the setting may affect whether you want to create several small custom requirements or a longer one that includes multiple steps.

You may find it helpful to set up a spreadsheet that represents your company's Host Integrity enforcement requirements.

## About Host Integrity requirements

The Host Integrity Policy includes the following requirement types:

- Predefined requirements cover the most common types of Host Integrity checks and allow you to choose from the following types:
  - Antivirus requirement
  - Antispyware requirement
  - Firewall requirement
  - Patch requirement
  - Service pack requirement
- Custom requirements, which you define by using the Custom Requirement Editor.  
See [“Writing a custom requirement script”](#) on page 573.
- Host Integrity requirement templates, which are updated as part of the Symantec Enterprise Protection online subscription service.  
See [“Adding a Host Integrity requirement from a template”](#) on page 553.

When you add a new requirement, you can select one of the predefined requirement types. A dialog box is then displayed with the set of predefined settings that you can configure. If the predefined settings do not meet your needs, you can create a custom requirement.

## Adding Host Integrity requirements

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

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

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

When you specify Host Integrity requirements, you can choose from the following types: predefined, custom, or template requirements. Template requirements are available through the Host Integrity Policy LiveUpdate service. You can copy and paste and export and import requirements between policies.

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

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

**To add a Host Integrity requirement**

- 1 In the console, open a Host Integrity Policy.  
See [“About editing policies”](#) on page 327.
- 2 On the Host Integrity Policy page, click **Requirements**.
- 3 On the Requirements page, select when the Host Integrity checks should run on the client from one of the following options:

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

- 4 Click **Add**.
- 5 In the Add Requirement dialog box, select one of the following requirement types:
  - Antivirus requirement
  - Antispyware requirement
  - Firewall requirement
  - Patch requirement
  - Service pack requirement
  - Custom requirement
- 6 Click **OK**.
- 7 Configure the settings for the requirement.  
See [“About Host Integrity requirements”](#) on page 549.

- 8 On the Advanced Settings page, configure settings for Host Integrity checks, remediation, and notifications.

For more information, click **Help**.

See [“About settings for Host Integrity checks”](#) on page 554.

- 9 When you are done with the configuration of the policy, click **OK**.
- 10 Assign the policy to groups or locations.

See [“Assigning a shared policy”](#) on page 329.

## Editing and deleting a Host Integrity requirement

The Requirements tab of the Host Integrity Setting dialog contains a table. You can use this table to add new requirements or you can edit or delete existing requirements from a Host Integrity Policy. You can double-click a requirement in the Requirements table to open it for editing. You can right-click in the Requirements table to add, edit, delete, move, import, export, copy, or paste requirements.

You may want to export a policy to a .dat file before editing. If the edited version of the policy does not function correctly, you can restore its original configuration by importing the .dat file. You must test a new policy or an edited policy in a safe environment.

### To edit and delete a Host Integrity requirement

- 1 In the console, open a Host Integrity Policy.  
See [“About editing policies”](#) on page 327.
- 2 On the Host Integrity page, click **Requirements**.
- 3 On the Requirements page, select a requirement and do one of the following options:
  - To edit a selected requirement, click **Edit**.
  - To permanently delete a selected requirement, click **Delete**, and then click **Yes**.
- 4 When you are done with the configuration of the policy, click **OK**.

## Enabling and disabling Host Integrity requirements

When you create requirements for a Host Integrity Policy, you can create requirements for future use. You must disable them from being used until they



are needed. You can disable a requirement temporarily while you test your Host Integrity Policy.

#### To enable and disable Host Integrity requirements

- 1 In the console, open a Host Integrity Policy.  
See [“About editing policies”](#) on page 327.
- 2 On the Host Integrity Policy page, click **Requirements**.
- 3 On the Requirements page, select a requirement, and then do one of the following tasks:
  - To enable a requirement, check the **Enable** check box for the selected requirement.
  - To disable a requirement, uncheck the **Enable** check box for the selected requirement.
- 4 When you are done with the configuration of the policy, click **OK**.

## Changing the sequence of Host Integrity requirements

You can change the position of requirements. When you change the position, you determine the order in which they are executed. The position can be important when you download the software that requires a restart after installation. You set the order to ensure that the requirements that require a restart for remediation are performed last.

#### To change the sequence of Host Integrity requirements

- 1 In the console, open a Host Integrity Policy.  
See [“About editing policies”](#) on page 327.
- 2 On the Host Integrity page, click **Requirements**.
- 3 On the Requirements page, select the requirement that you want to move, and then click **Move Up** or **Move Down**.
- 4 When you are done with the configuration of the policy, click **OK**.

## Adding a Host Integrity requirement from a template

The online subscription service provides Host Integrity templates.

You can import the latest templates and use them while you develop custom requirements for a Host Integrity Policy. You can select as many or as few requirements as you want. You can select the requirement by using them as is or by modifying them as needed for your environment.

If your subscription is expired, the requirements that you already imported still can be used. However, the latest updates are no longer available to import.

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 Host Integrity requirement from a template

- 1 In the console, open a Host Integrity Policy.  
See [“About editing policies”](#) on page 327.
- 2 On the Host Integrity page, click **Requirements**.
- 3 On the Requirements page, click **Template**.
- 4 In the Host Integrity Online Updating dialog box, expand Templates, and then select a template category.
- 5 Next to each template you want to add, click **Add**.
- 6 Click **Import**.
- 7 When you are done with the configuration of the policy, click **OK**.

## About settings for Host Integrity checks

When you set up Host Integrity Policies, you can select from a number of settings. The settings relate to how the Host Integrity check is carried out and how the results are handled.

If you change a Host Integrity Policy, it is downloaded to the client at the next heartbeat. The client then runs a Host Integrity check.

If the user switches to a location with a different Host Integrity Policy while a Host Integrity check is in progress, the client stops the check. The stop includes remediation attempts, if required by the policy. The user may get a timeout message if a remediation server connection is not available in the new location. When the check is complete, the client discards the results. Then the client immediately runs a new Host Integrity check based on the new policy for the location.

If the policy is the same in the new location, the client maintains any Host Integrity timer settings. The client runs a new Host Integrity check only when required by the policy settings.

[Table 40-1](#) displays the settings for Host Integrity checks.

**Table 40-1** Host Integrity checking settings

Setting	Description
Check Host Integrity every	Specifies the frequency of Host Integrity checks.
Keep check results for	<p>Sets the duration for maintaining Host Integrity results.</p> <p>You can set the amount of time that a client retains the result of a previous Host Integrity check. The client maintains the result even if the user takes an action that would normally result in a new Host Integrity check. For example, the user may download new software or change a location.</p>
Continue to check requirements after one fails	<p>Specifies that the client continues to check the requirements even if one requirement fails. The client does stop the Host Integrity check until the failed requirement is restored.</p> <p>The client checks the Host Integrity requirements in the order that is specified in the Host Integrity Policy.</p> <p>If you enable this setting, the Host Integrity check fails, but you can try other remediation actions, if required.</p> <p>You can allow the Host Integrity check to pass even if a requirement fails. This setting is found on the Requirements dialog box for each requirement type. You apply the setting separately for each requirement.</p>

## Setting up logging and notifications for a Host Integrity check

When the client runs a Host Integrity check, it logs the result of each requirements check and displays the results in the client's Security log. Although you need this information when troubleshooting, you may not want users to have access to detailed logging information. For example, you may not want registry keys and file name information to appear. Any Host Integrity requirements that have either passed or failed are listed. The details are recorded in the log and can be viewed from the management server Monitors page.

You can also configure notifications to appear on the client when the following conditions occur:

- A Host Integrity check fails.
- A Host Integrity check passes after it previously failed.  
For example, if the Host Integrity check fails and the client restores the required software so that the Host Integrity check then passes, the following message can appear when the check passes:

```
Host Integrity check passed.
```

Other notifications may appear on the client computer in the following situations:

- If you allow the user to cancel the remediation for a requirement, a notification gives the user the choice to download the software immediately or postpone the remediation.
- If an Enforcer is running and the Host Integrity check fails, you can specify whether the client displays a notification that notifies the user that the Enforcer has blocked network access. To enable or disable this notification for the client and to add text, click the Policies page, select the group in the View Policies pane, click General Settings, and then the Security Settings.

See [“Allowing users to postpone or cancel Host Integrity remediation”](#) on page 560.

#### To set up logging and notifications for a Host Integrity check

- 1 In the console, open a Host Integrity Policy.  
See [“About editing policies”](#) on page 327.
- 2 On the Host Integrity page, click **Advanced Settings**.
- 3 On the Advanced Settings page, under Notifications, click any of the following options:
  - To display detailed information in the client, click **Show verbose Host Integrity Logging**.
  - **Display a notification message when a Host Integrity check fails.**
  - **Display a notification message when a Host Integrity check passes after previously failing.**
- 4 To add a custom message, click **Set Additional Text**, and then type up to 512 characters of additional text.
- 5 When you are finished with the configuration of this policy, click **OK**.

## Allowing the Host Integrity check to pass if a requirement fails

In addition to enabling or disabling a requirement on your Host Integrity Policy to determine whether or not the client runs the requirement script, you can have

the client run the requirement script and log the results but ignore the results. You can let the Host Integrity check pass whether or not the requirement fails. A requirement can pass even if the requirement condition is not met.

You enable Allow the Host Integrity check to pass even if the requirement fails on the dialog for a specific requirement. If you want to apply this setting to all requirements, you must enable the setting on each requirement separately. The setting is disabled by default.

If you enable the setting to allow the Host Integrity check to pass even if the requirement fails, the following message appears in the client window when the event occurs:

```
Host Integrity failed but reported as pass
```

#### To allow the Host Integrity check to pass if a requirement fails

- 1 In the console, open a Host Integrity Policy.  
See [“About editing policies”](#) on page 327.
- 2 On the Host Integrity page, click **Requirements**.
- 3 On the Requirements page, click **Add**, add a predefined requirement or a custom requirement, and then click **OK**.
- 4 On the dialog box for the requirement, check **Allow the Host Integrity check to pass even if this requirement fails**.
- 5 Click **OK**.
- 6 When you finished with the configuration of this policy, click **OK**.

## About Host Integrity remediation

If the client Host Integrity check shows that the Host Integrity requirements are not met, the client can try to restore the files. The client computer then needs to pass the Host Integrity check. The client downloads, installs files, or starts required applications. When you set up Host Integrity Policies, you can specify what happens during the remediation process. You can specify not only where the client goes to download remediation files but also how the remediation process is implemented.

You can allow the user to cancel a remediation download. You can also set the number of times the user can postpone a download and for how long. The settings apply to all types of requirements in the policy except those on which you have disabled canceling remediation. Users can cancel only predefined requirements.

By default, Host Integrity remediation runs whether or not the user is logged on. This enables the client computer to be remediated with operating system updates

or necessary security software at any time. However, when the remediation runs either a local program or a downloaded program, users may be able to open and run the program before they have logged on. For example, an installation package might launch Internet Explorer, from which users can run either the command prompt or another program. You can work around this issue when you write a custom requirement that uses the Run a program function. You cannot work around this issue for predefined requirements.

See [“Running a program”](#) on page 578.

## About restoring applications and files for Host Integrity

When you set up remediation for a requirement, you specify the location of an installation package or files to be downloaded and installed. When you specify the location of the installation package or file to be downloaded, you can use any of the following formats:

UNC            \\servername\sharename\dirname\filename

UNC restore does not work if Network Neighborhood browsing is disabled on the target client. Be certain that Network Neighborhood browsing has not been disabled if you use UNC paths for remediation.

FTP            FTP://ftp.ourftp.ourcompany.com/folder/filename

HTTP          HTTP://www.ourwww.ourcompany.com/folder/filename

Installation packages or files are always downloaded to the temporary directory. Any relative path refers to this directory. The temporary directory is defined in the TMP environment variable if it exists, or in the TEMP environment variable if that exists. The default directory is in the Windows directory.

For file execution, the current working directory is always set to the Windows temporary directory. Environment variables are substituted before execution. The Windows directory path replaces the command %windir%.

You can use %1 (the default) to execute the file you specified in the Download URL field. The %1 variable represents the last downloaded file.

After the download, installation, or execution of a command to restore a requirement, the client always retests the requirement. Also, the client logs the results as pass or fail.

## Host Integrity remediation and Enforcer settings

When you set up Host Integrity requirements, you can specify that if the Host Integrity requirements are not met, the client should update the client computer

with whatever is required by connecting to a remediation server. If you apply such requirements to clients that connect to the network through an Enforcer, you must ensure that the client, while blocked from regular network access, can access the remediation server. Otherwise, the client does not restore Host Integrity and the client continues to fail the Host Integrity requirement.

How you accomplish this task depends on the type of Enforcer. The following list offers a few examples:

- For the Gateway Enforcer, you can configure the Gateway Enforcer to recognize the remediation server as a trusted internal IP address.
- For the DHCP Enforcer, you set up the quarantine network configuration on the DHCP server to allow access to the remediation server.
- For a LAN Enforcer, if you use a switch with dynamic VLAN capability, you can set up a VLAN with access to the remediation server.

## Specifying the amount of time the client waits to remediate

You can specify the amount of time the client waits before it tries to install and start the remediation download again. Regardless of the time that you specify, whenever a new Host Integrity check is initiated, the client tries to remediate the client computer again.

### To specify the amount of time the client waits to remediate

- 1 In the console, open a Host Integrity Policy.  
See [“About editing policies”](#) on page 327.
- 2 On the Host Integrity Policy page, click **Requirements**.
- 3 On the Requirements page, click **Add**, add a predefined requirement, and then click **OK**.
- 4 On the dialog box for each predefined requirement, check **Install requirement name if it has not been installed on the client**.
- 5 Check **Download Installation Package**.  
For the Antivirus requirement, check **Download the installation package**.
- 6 Check **Specify wait time before attempting the download again if the download fails**.
- 7 Specify the amount of time to wait by the minutes, hours, or days.
- 8 When you are done with the configuration of the policy, click **OK**.

## Allowing users to postpone or cancel Host Integrity remediation

If a requirement specifies a remediation action, you can allow the user to cancel the remediation. Or, you can allow the user to postpone the remediation to a more convenient time. Examples of remediation actions include the installation of an application or an update of a signature file. You can set a limit on how many times a remediation can be canceled and how long the user can postpone it. The limits you set determine the selections available to the user on the pop-up window that the client displays when remediation is needed. You can also add text to the pop-up window.

The minimum and the maximum time settings determine the range of choices available on the pop-up window. The pop-up window displays to a user when a requirement fails. The range appears as a list next to the Remind me later icon on the pop-up message.

If the user selects a shorter time for postponement than the Host Integrity check frequency, the user selection is overridden. The pop-up window does not appear again until the client runs another Host Integrity check. If the user has chosen to be reminded in 5 minutes, but the Host Integrity check runs every 30 minutes, the remediation pop-up window does not appear until 30 minutes have passed. To avoid confusion for the user, you may want to synchronize the minimum time setting with the Host Integrity check frequency setting.

If the user postpones remediation, the client logs the event. The Host Integrity is shown as failed since the requirement is not met. The user can manually run a new Host Integrity check at any time from the client user interface.

If the user has postponed a remediation action and in the interim the client receives an updated policy, the amount of time available for remediation is reset to the specified maximum.

### To allow users to postpone Host Integrity remediation

- 1 In the console, open a Host Integrity Policy.  
See [“About editing policies”](#) on page 327.
- 2 On the Host Integrity Policy page, click **Advanced Settings**.
- 3 On the Advanced Settings page, under Remediation Dialog Options, set a minimum time limit and the maximum time limit that a user can postpone the remediation.
- 4 Type the maximum number of times that the user can cancel the remediation.



- 5 To add a custom message on the client computer, click **Set Additional Text**.  
The message you type is displayed on the client pop-up remediation window if the user clicks the Details option. If you specify no additional text, the default pop-up window text is repeated in the Details area when the user clicks Details.
- 6 In the Enter Additional Text dialog box, type a custom message up to 512 characters, and then click **OK**.
- 7 When you are done with the configuration of the policy, click **OK**.

#### To allow users to cancel Host Integrity remediation

- 1 In the console, open a Host Integrity Policy.  
See [“About editing policies”](#) on page 327.
- 2 On the Host Integrity Policy page, click **Requirements**.
- 3 On the Requirements page, click **Add**, add a predefined requirement, and then click **OK**.
- 4 On the dialog box for each predefined requirement, check **Install requirement name if it has not been installed on the client**.
- 5 Check **Download Installation Package**.  
For the Antivirus requirement, check **Download the installation package**.
- 6 Check **Allow the user to cancel the download for Host Integrity remediation**.
- 7 When you are done with the configuration of the policy, click **OK**.

**Allowing users to postpone or cancel Host Integrity remediation**

# Adding custom requirements

This chapter includes the following topics:

- [About custom requirements](#)
- [About conditions](#)
- [About functions](#)
- [About custom requirement logic](#)
- [Writing a custom requirement script](#)
- [Displaying a message dialog box](#)
- [Downloading a file](#)
- [Generating a log message](#)
- [Running a program](#)
- [Running a script](#)
- [Setting the timestamp of a file](#)
- [Specifying a wait time for the script](#)

## About custom requirements

Custom requirements check a client computer for any number of administrator-selected or defined criteria. You can write custom requirements to remediate any identified compliancy issues.

You can create a complex or a simple requirement script by using predefined selections and fields.

The fields and lists that are available in the predefined requirement dialog boxes are available when you create custom requirements. However, custom requirements give you more flexibility. In custom requirements, you can add the applications that are not included in the predefined lists of applications. You can create subsets of predefined lists by adding each application individually.

## About conditions

Conditions are the checks that may be performed within a custom requirement script to detect compliancy issues.

You can chose from the following categories of conditions:

- Antivirus checks
- Antispyware checks
- Firewall checks
- File checks and operation
- Registry checks and operations
- Utilities

You can specify conditions as present or absent (NOT). You can include multiple condition statements by using AND or OR keywords.

## About antivirus conditions

In a custom requirement, you can specify antivirus applications and signature file information to check as part of your IF-THEN condition statement.

You can check for the following conditions:

- Antivirus is installed
- Antivirus is running
- Antivirus signature file is up to date

When you check applications and signature files as part of a custom requirement, you specify the same information as when you create a predefined requirement. The option names may differ slightly.

If you select Any Antivirus Product, any of the applications in the drop-down list meet the requirement. You can include a subset of applications by selecting each by using the OR keyword.

When you specify the signature file information, you can select one or both options for checking that the signature file is up to date. If you select both, the following conditions must be satisfied to meet the requirement:

- Select Check signature file is less than and enter a number of days. A file that is dated before the number of days you specify is out of date.
- Select Check signature file date is and select before, after, equal to, or not equal to, and specify a date (mm/dd/yyyy). Optionally, specify an hour and minute; the default is 00:00. The file's last modified date determines the signature file age.

## About antispyware conditions

For a custom Host Integrity requirement, you can specify Antispyware applications and signature file information to check as part of your IF THEN condition statement.

You can check for the following conditions:

- Antispyware is installed
- Antispyware is active
- Antispyware signature file is up to date

When you check applications and signature files as part of a custom requirement, you can specify the same information as when you create a predefined requirement. The option names may differ slightly.

If you select the Any Antispyware Product, any of the applications in the drop-down list meet the requirement.

When you specify the signature file information, you can select one or both options for checking that the signature file is up to date. If you select both options, both of the following conditions must be satisfied to meet the requirement:

- Select Check signature file is less than and enter a number of days.  
A file that is dated before the number of days you specify is out of date.
- Select Check signature file date is and select before, after, equal to, or not equal to, and specify a date (mm/dd/yyyy). Optionally, specify an hour and minute; the default is 00:00. The file's last modified date determines the signature file age.

## About firewall conditions

For a custom Host Integrity requirement, you can specify firewall applications to check as part of your IF-THEN condition statement.

You can check for the following conditions:

- Firewall is installed
- Firewall is running

If you want to select any of the applications in the drop-down list, you can select Any Firewall Product. You can include a subset of applications by selecting each using the OR keyword.

## About file conditions

For a custom Host Integrity requirement, you can check an application or a file as part of your IF-THEN condition statement.

You can specify the following options to check file information in a custom Host Integrity requirement:

File: Compare file age to	Specify a number of days or weeks and select greater than or less than.
File: Compare file date to	Specify a date in the format mm/dd/yyyy. Optionally, specify an hour and minute. The default time is 00:00. You can select equal to, not equal to, before, or after.
File: Compare file size to	Specify the number of bytes. You can select equal to, not equal, less than, or greater than.
File: Compare file version to	Specify a file version in the format x.x.x.x, where x represents a decimal number from 0 to 65535. You can select equal to, not equal, less than, or greater than.
File: File exists	Specify the name of the file to be checked for.
File: File fingerprint equals	Normally you get this information by selecting an application using Search for Applications.
Specify a hexadecimal number (up to 32 digits)	When you select an option, additional fields appear on the dialog. For each option you specify the file name and path and you enter the additional information that is required.

File: File Download complete

You can download a file from a location that you specify to a directory that you specify. If authentication is required to access a file location by HTTP, you can specify the user name and password.

You can use system variables, registry values, or a combination of them to specify the file name and path. When you select one of the file options, the dialog shows examples of ways to enter the file name and path.

You can locate the applications that have been recorded by using the Search for Applications feature. When you specify file options in the custom requirement script, the Search for Applications option provides access to the same search tool as the Search for Applications tool. You can browse the groups that are defined in the management server to filter the applications, enter a search query, and export the results to a file.

To search using system environment variables or registry values:

To use the system environment variable

To specify the file named cmd.exe located under the directory that is specified in the WINDIR environment variable, type the following command:

```
%WINDIR%\cmd.exe
```

To use the registry value

To read the value HKEY\_LOCAL\_MACHINE\Software\Symantec\AppPath as the path of the file sem.exe, type the following command:

```
#HKEY_LOCAL_MACHINE\  
Software\Symantec\AppPath#\br/>sem.exe
```

To use the combined registry and system environment variable

Use the following example to use the combined registry value and system environment variable:

```
%SYSTEMDIR%\br/>#HKEY_LOCAL_MACHINE\  
Software\Symantec\AppPath#.
```

## About operating system conditions

For a custom Host Integrity requirement, you can specify operating system information to check as part of your IF-THEN condition statement. When you select an option, additional fields appear on the dialog.

Utility: Operating system is Specify an operating system. When you want to update a patch, you need to select the exact versions that require that patch. You can use the OR keyword to specify more than one operating system.

Utility: Operating system language is The function detects the language version of the client's operating system. If the language version is not listed in the Custom Requirement dialog, you can add languages by typing their identifiers in the Language Identifiers field. To add multiple identifiers, use a comma to separate each ID such as 0405,0813. See the Language Identifiers table for the list of identifiers.

Patch: Compare current service pack with specified version Type the number of the service pack that you want to check for, such as 1a. The number is limited to two characters. You can check for the following conditions: equal to, not equal to, less than, or greater than.  
  
A number that is followed by a letter is considered greater than the number alone; for example, service pack number 6a is considered greater than 6. Be sure to apply patches one at a time.

Patch: Patch is installed Type the patch name that you want to check for. For example: KB12345. You can type only numbers and letters in this field.

Be sure to match the patch name or service pack number with the correct version of the operating system. If you specify an operating system that does not match the patch or the service pack, the requirement fails.

## About registry conditions

For a custom Host Integrity requirement, you can specify registry settings to check as part of your IF-THEN condition statement. You can also specify ways to change registry values. Only HKEY\_LOCAL\_MACHINE, HKEY\_CLASSES\_ROOT, and HKEY\_CURRENT\_CONFIG are supported registry settings.



The following selections are available for checking registry settings:

Registry: Registry key exists	Specify a registry key name to check whether it exists.
Registry: Registry value equals	Specify a registry key name and a value name and specify what data to compare the value against.
Registry: Registry value exists	Specify a registry key name to check if it has the specified value name.
Registry: Set registry value	Specify a value to assign for the specified key; if the key does not exist, it creates the key. This selection replaces an existing value, whether or not it is of the same type; in other words, if the existing value is a DWORD value but you specify a string value, it replaces the DWORD with the string value.
Registry: Increment registry DWORD value	Specify a DWORD value. This selection lets you perform counts, such as allowing an unpatched computer to meet the requirement no more than n times.

When you specify registry keys, remember the following considerations:

- The key name is limited to 255 characters.
- If the registry key has a backslash (\) at the end, it is interpreted as a registry key. For example: `HKEY_LOCAL_MACHINE\SOFTWARE\`
- If the registry key has no backslash at the end, then it is interpreted as a registry name. For example: `HKEY_LOCAL_MACHINE\SOFTWARE\ActiveTouch`

When you specify registry values, remember the following considerations:

- The value name is limited to 255 characters.
- You can check for values as DWORD (decimal), binary (hexadecimal), or string.
- For DWORD values, you can check whether the value is less than, equal to, not equal to, or greater than the specified value.
- For string values, you can check whether the value data equals or contains a given string. If you want the string comparison to be case-sensitive, check the Match case check box.
- For binary values, you can check whether the value data equals or contains a given piece of binary data. Hexadecimal bytes represent the data. If you specify value contains, you can also specify the offset for this data. If the offset is left

blank, it searches the value for the given binary data. Allowed values for the hexadecimal edit box are 0 through 9 and a through f.

The following are examples of registry values:

DWORD	12345 (in decimal)
Binary	31 AF BF 69 74 A3 69 (in hexadecimal)
String	ef4adf4a9d933b747361157b8ce7a22f

## About functions

You use functions to define the actions that are performed when a conditional expression is evaluated as true or false.

A custom requirement condition can check for the installation of a particular antivirus product, but it cannot be configured to install the product as a remediation action. When you write custom requirements, you must explicitly define the remediation actions to be performed by using function statements.

Functions appear within THEN and ELSE statements, or may appear at the end of a custom requirement script. To achieve a desired remediation result, you may need to specify multiple functions. Each function performs a very specific task, such as to download a file or to execute a file. You do not define individual functions to provide specific remediation actions, such as to install a specific antivirus product. To download a specific antivirus product, you must use the general download function.

[Table 41-1](#) displays the following functions in a custom requirement script:

**Table 41-1** Custom requirement functions

Function	Description
Download a file	Downloads a file that is referenced by a URL or UNC to the client computer. If a URL is used, both HTTP and FTP are supported.
Set registry value Increment registry DWORD value	Creates and then sets or increments a registry value contained within a specified registry key.
Log message	Specifies a custom message to be added to the client Security log and the registry.

**Table 41-1** Custom requirement functions (*continued*)

Function	Description
Run a program	Executes a program that is already resident on the client computer. The program may be executed under the system context or the current logged-in user context.
Run a script	Runs a custom script on the client computer. You can use the built-in text editor to create the script contents. The script may be a batch file, an INI file, or any executable format that is recognized by Windows. Additionally, the script may simply contain parameters to be provided to another program.
Set Timestamp	Stamps a specified file on the client computer with the current time and date.
Show message dialog	Displays a message dialog window on the client computer with an OK button. A default timeout may be specified.
Wait	Pauses execution of the custom requirement script for a specified period.

## About custom requirement logic

You write the custom requirements by using the script-like logic. The rules use IF..THEN..ELSE logic from a list on predefined conditions and actions.

### About the RETURN statement

You can add a RETURN statement to specify the overall Host Integrity result of the requirement. The RETURN statement includes the PASS keyword and the FAIL keyword. All custom requirements must include a RETURN statement at the end.

Unlike a predefined requirement, a custom requirement must explicitly specify what the result of the Host Integrity check will be. In some cases, the evaluation of a set of conditions as being true should be interpreted as the custom requirement passing Host Integrity evaluation. In other cases, you may want the same evaluation to be interpreted as failing Host Integrity evaluation.

### About the IF, THEN, and ENDIF statement

You can define the primary logic structure of a custom requirement by one or more IF, THEN, and ENDIF statements. An IF, THEN, and ENDIF statement defines

a structure in which specific conditions are checked (IF), and the actions that are taken when those conditions are evaluated as being true (THEN).

You can nest IF, THEN, and ENDIF statements to form more complex custom requirements. You must nest the IF, THEN, and ENDIF statements whenever one condition must be true before another condition can be evaluated.

## About the ELSE statement

An IF, THEN, and ENDIF statement is limited to a set of conditions and a set of actions that are executed when the conditions are evaluated as being true. In many cases, you may need to specify one or more actions to be taken to perform a desired remediation action. You may add an ELSE statement to identify the actions to be taken whenever the specified conditions are evaluated as being false.

## About the NOT keyword

You can use the NOT keyword to reverse the logical evaluation of a particular condition. After a condition has been added to the custom requirement script, you can right-click the condition and select Toggle NOT to reverse the logical of the condition. The use of the NOT keyword does not change the overall true and false evaluation of the IF statement. It reverses only the true and false state of a particular condition.

## About AND, OR keywords

You can specify multiple conditions within an IF, THEN, or ENDIF statement; however, additional keywords must be added to accomplish this. Within any IF statement, you can add the AND OR keywords to logically associate multiple conditions. The logical association of the conditions directly affects the overall true or false evaluation of the IF statement. If you use the AND keyword in an IF statement, all the conditions in the IF statement must be evaluated as true for the IF statement to be true. If you use the OR keyword, only one of the conditions in the IF statement must be evaluated for the IF statement to be true.

When you specify multiple conditions, you must interpret the logical association of the conditions to anticipate what the correct true or false evaluation should be. The custom requirement script does not display the expression with a parenthesis format, but with nested keywords and nodes. The first expression always begins with the first condition specified, and continues as long as the same logical operator keyword is used. For example, you can use the OR keyword to associate three different conditions. As long as you use the OR keyword, all the conditions are contained within the same logical expression.

## Writing a custom requirement script

To build a custom requirement, you add one or more IF.THEN.. statements to a script. When you run the script, the Host Integrity check looks for the condition that is listed under the IF node. Depending upon the condition, the action that is listed under the THEN node is executed. The result (pass or fail) is returned.

The script displays a tree structure in the left pane and a drop-down list of conditions or functions in the right pane.

As part of a custom requirement, you can specify whether to allow the Host Integrity check to pass if the requirement fails. When you plan how many different conditions to check for in one script, remember that this setting applies to the custom requirement script as a whole. This choice may affect whether you want to create several small custom requirements or a longer one that includes multiple steps.

### To write a custom requirement script

- 1 Add a custom requirement.  
See [“Adding Host Integrity requirements”](#) on page 550.
- 2 In the Custom Requirement dialog box, type a name for the requirement.  
The requirement name can appear on the client computer. The name notifies the user whether the requirement passed or failed or prompts the user to download the software.
- 3 To add a condition, under Customized Requirement Script, click **Add**, and then click **IF.THEN...**
- 4 With the highlight on the empty condition under the IF node, in the right pane, select a condition.  
The Host Integrity check looks for the condition on the client computer.
- 5 Under the Select a condition drop-down list, specify the additional information that is required.
- 6 Under Customized Requirement Script, click **THEN**, and then click **Add**.  
The THEN statement provides the action that should be taken if the condition is true.
- 7 Click any of the following options:
  - **IF.. THEN**  
Use a nested IF.. THEN.. statement to provide additional conditions and actions.  
See [“Adding an IF THEN statement”](#) on page 574.

- **Function**  
Use a function to define a remediation action.  
See [“About functions”](#) on page 570.
  - **Return**  
Use a return statement to specify whether the results of the evaluation of the condition passes or fails. Every custom requirement must end with a pass or fail statement.
  - **Comment**  
Use a comment to explain the functionality of the conditions, functions, or statements that you are adding.  
See [“Adding a comment”](#) on page 575.
- 8** In the right-hand pane, define the criteria that you added.  
For more information on these options, click **Help**.
  - 9** To add more nested statements, conditions, or functions, under Customized Requirement Script, right-click the node, and then click **Add**.
  - 10** Repeat steps **7** to **8** as needed.
  - 11** To allow the Host Integrity check to pass no matter what the result, check **Allow the Host Integrity check to pass even if this requirement fails**.
  - 12** When you are done with the configuration of the requirement, click **OK**.

## Adding an IF THEN statement

An IF..THEN statement defines a structure in which specific conditions are checked (IF), and the actions that are taken when those conditions are evaluated as being true (THEN).

### To add an IF THEN statement

- 1** Write a custom requirement script.  
See [“Writing a custom requirement script”](#) on page 573.
- 2** Under Customized Requirement Script, select one of the following:
  - To add the first IF THEN statement, select the top node.
  - To add an IF THEN statement at the same level as an existing one, select **END IF**.
  - To add a nested IF THEN statement, select the line under which you want to add it.

- 3 Click **Add**.
- 4 Click **IF..THEN**.

## Switching between the IF statement and the IF NOT statement

You may need to change between checking for the presence or absence of a condition.

### To change between the IF statement and the IF NOT statement

- 1 Write a custom requirement script.  
See [“Writing a custom requirement script”](#) on page 573.
- 2 Right-click the condition, and then click **Toggle NOT**.

## Adding an ELSE statement

You may add an ELSE statement to identify the actions to be taken whenever the specified conditions are evaluated as being false.

### To add an ELSE statement

- 1 Write a custom requirement script.  
See [“Writing a custom requirement script”](#) on page 573.
- 2 Under Customized Requirement Script, click **THEN**.
- 3 Click **Add**, and then click **ELSE**.

## Adding a comment

When you add a statement, such as an IF THEN statement, you can add a comment. Use the comment to explain what that part of the code is supposed to do. The comments are for informational purposes only.

### To add a comment

- 1 Write a custom requirement script.  
See [“Writing a custom requirement script”](#) on page 573.
- 2 Under Customized Requirement Script, select any statement that you have already added, and then click **Add**.
- 3 Click **Comment**.
- 4 Click **//Insert statements here**, and in the right-hand pane, in the Comment text field, enter your comments.

## Copying and pasting IF statements, conditions, functions, and comments

You can copy and paste statements or entire IF THEN nodes within or between custom requirements. You may want to copy and paste these elements if you want to move them to another part of the script or to repeat the functionality.

### To copy and paste an IF statement

- 1 Write a custom requirement script.  
See [“Writing a custom requirement script”](#) on page 573.
- 2 Under Customized Requirement Script, right-click the script element, and then click **Copy**.
- 3 Right-click an empty statement line, and then click **Paste**

## Deleting a statement, condition, or function

You can delete statements, conditions, or functions at any time. If there is only one condition statement under an IF node, deleting it deletes the entire IF THEN statement.

### To delete a statement, condition, or function

- 1 Write a custom requirement script.  
See [“Writing a custom requirement script”](#) on page 573.
- 2 Under Customized Requirement Script, select the requirement element that you want to delete.
- 3 Click **Delete**.
- 4 If asked to confirm the deletion, click **Yes**.

## Displaying a message dialog box

In the custom Host Integrity requirement, you can specify a function or a condition that creates a message box for the client to display to the user. The function or the condition returns true if the user clicks OK or Yes. Otherwise it returns false.

### To display a message dialog box

- 1 Write a custom requirement script.  
See [“Writing a custom requirement script”](#) on page 573.
- 2 In the Custom Requirement dialog box, under Custom Requirement Script, select the node where you want to add the function.



- 3 Click **Add**, and then click **Function**.
- 4 Click **Utility: Show message dialog**.

To insert a condition, select **IF...Then**, and then select the appropriate branch. Then select **Utility: Message dialog return value equals**.
- 5 Type a caption for the message box, up to 64 characters.
- 6 Type the text for the message box up to 480 characters.
- 7 Select one of the following icons to display: Information, Question, Warning, or Error.

Both the icon and the text appear.
- 8 Select the set of buttons that appear in the dialog box:
  - OK
  - OK and Cancel
  - Yes and No
- 9 Select the default button for each set of buttons.
- 10 To close the message box and return a default value after a certain time with no user interaction, check **Action to take to dismiss message box after maximum waiting time**, and specify the wait time.

The time value must be greater than 0.

## Downloading a file

For a custom requirement, you can specify that a file is downloaded to the client computer.

### To download a file

- 1 Write a custom requirement script.

See [“Writing a custom requirement script”](#) on page 573.
- 2 In the Custom Requirement dialog box, under Custom Requirement Script, select the node where you want to add the function.
- 3 Click **Add**, and then click **Function**.
- 4 Click **Utility: Download a file**.

- 5 Enter the URL location that the file is downloaded from, and the folder on the client computer you want the file to be downloaded to.

You can specify the location by a URL or a UNC. If you use a URL, both HTTP and FTP are supported.

- 6 Check **Show the download process dialog** so that the users can watch the file as the file gets downloaded to the client computer.
- 7 If you want the user to be able to cancel the file download, check **Allow the user to cancel Host Integrity for this requirement**.

Users may lose work if the file is downloaded at the wrong time.

## Generating a log message

In the custom Host Integrity requirement, you can specify a function to log a message about an action. This function inserts the specified message string into the client Security log. The message appears in the details area of the Security log.

### To generate a log message

- 1 Write a custom requirement script.  
See [“Writing a custom requirement script”](#) on page 573.
- 2 In the Custom Requirement dialog box, under Custom Requirement Script, select the node where you want to add the function.
- 3 Click **Add**, and then click **Function**.
- 4 Click **Utility: Log message**.
- 5 In the Severity Type drop-down list, select one of the following log severity types: Information, Major, Minor, or Critical.
- 6 Type a message up to 512 characters long.

## Running a program

For a custom Host Integrity requirement, you can specify a function to have the client launch a program.

### To run a program

- 1 Write a custom requirement script.  
See [“Writing a custom requirement script”](#) on page 573.
- 2 In the Custom Requirement dialog box, under Custom Requirement Script, select the node where you want to add the function.
- 3 Click **Add**, and then click **Function**.
- 4 Click **Utility: Run a program**.
- 5 In the Execute the command text field, type the command to execute the script.

Environment variables are substituted before execution. For example, `%windir%` is replaced by the Windows directory path. You can use the `%1` variable to execute the last downloaded file.

- 6 Under Run a Program, select one of the following options:
  - in system context
  - in logged-in user context  
The Execute command must include the whole file path, thus showing who the logged-in user is. If no user is logged in, the result fails.
- 7 To specify the amount of time to allow the execute command to complete, select one of the following options:
  - Do not wait  
The action returns true if the execution is successful but it does not wait until the execution is completed.
  - Wait until execution completes
  - Enter maximum time  
Enter a time in seconds. If the Execute command does not complete in the specified time, the file execution is terminated.
- 8 Optionally, uncheck **Show new process window**.

## Running a script

In the custom Host Integrity requirement, you can specify a function that causes the client to run a script. You can use a scripting language, such as JScript or VBScript, which you can run with the Microsoft Windows Script Host.

### To run a script

- 1 Write a custom requirement script.  
See “[Writing a custom requirement script](#)” on page 573.
- 2 In the Custom Requirement dialog box, under Custom Requirement Script, select the node where you want to add the function.
- 3 Click **Add**, and then click **Function**.
- 4 Click **Utility: Run a script**.
- 5 Enter a file name for the script, such as `myscript.js`.
- 6 Type the content of the script.
- 7 In the Execute the command text field, type the command to execute the script.  
Use `%F` to specify the script file name. The script is executed in system context.
- 8 To specify the amount of time to allow the execute command to complete, select one of the following options:
  - **Do not wait**  
The action returns true if the execution is successful but it does not wait until the execution is completed.
  - **Wait until execution completes**
  - **Enter maximum time**  
Enter a time in seconds. If the Execute command does not complete in the specified time, the file execution is terminated.
- 9 Optionally uncheck **Delete the temporary file after execution is completed or terminated**.  
This option is disabled and unavailable if Do not wait is selected.
- 10 Optionally uncheck **Show new process window**.

## Setting the timestamp of a file

In the custom requirement, you can specify the Set Timestamp function to create a 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.

One example is if you have set the Host Integrity check to run at a short interval such as 2 minutes and you want to specify an action to occur at a longer interval

such as when a day. In this case, the stored time value is removed when the client receives a new profile or when the user manually runs a Host Integrity check.

#### To set the timestamp of a file

- 1 Write a custom requirement script.  
See [“Writing a custom requirement script”](#) on page 573.
- 2 In the Custom Requirement dialog box, under Custom Requirement Script, select the node where you want to add the function.
- 3 Click **Add**, and then click **Function**.
- 4 Click **Utility: Set Timestamp**.
- 5 Type a name up to 256 characters long for the registry setting that stores the date and the time information.

#### To compare the current time to the stored time value

- 1 Write a custom requirement script.  
See [“Writing a custom requirement script”](#) on page 573.
- 2 In the Custom Requirement dialog box, under Custom Requirement Script, select the node where you want to add the condition.
- 3 Click **Add**, and then click **IF.THEN...**
- 4 Click **Utility: Check Timestamp**.
- 5 Type the name you entered for the saved time registry setting.
- 6 Specify an amount of time in minutes, hours, days, or weeks.  
If the specified amount of time has passed, or if the value of the registry setting is empty, the Set Timestamp function returns a value of true.

## Specifying a wait time for the script

In the custom Host Integrity requirement, you can specify a function that causes the custom requirement script to wait for a specified length of time before it runs.

#### To specify a wait time for the script

- 1 Write a custom requirement script.  
See [“Writing a custom requirement script”](#) on page 573.
- 2 In the Custom Requirement dialog box, under Custom Requirement Script, select the node where you want to add the function.
- 3 Click **Add**, and then click **Function**.

- 4** Click **Utility: Wait**.
- 5** Type the number of seconds to wait.

# Using the command-line interface

This appendix includes the following topics:

- [The client service](#)

## The client service

You can manipulate the client directly from the command line on the client computer by using the `smc` command for the client service. You may want to use this command in a script that runs the parameters remotely. For example, if you need to stop the client to install an application on multiple clients, you can stop and restart each client service.

With the exception of `smc -start`, the client service must run to use the command-line parameters. The command-line parameters are not case-sensitive.

[Table A-1](#) describes the parameters that you can run if users are members of any Windows user group.

**Table A-1** Parameters that all Windows members can use

Parameter	Description
<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

**Table A-1** Parameters that all Windows members can use (*continued*)

Parameter	Description
smc -dismissgui	<p>Closes either the Symantec Endpoint Protection or Symantec Network Access Control client user interface, including the notification area icon.</p> <p>The client still runs and protects the client computer.</p> <p>Returns 0</p>
smc -exportlog	<p>Exports the entire contents of a log to a .txt file.</p> <p>To export a log, 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"> <li>■ 0 = System Log</li> <li>■ 1 = Security Log</li> <li>■ 2 = Traffic Log</li> <li>■ 3 = Packet Log</li> <li>■ 4 = Control Log</li> </ul> <p>For example, you might type:</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 only export 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>
smc -runhi	<p>If Symantec Network Access Control is installed, runs a Host Integrity check.</p> <p>Returns 0</p>
smc -showgui	<p>Displays either the Symantec Endpoint Protection or the Symantec Network Access Control client user interface.</p> <p>Returns 0</p>



**Table A-1** Parameters that all Windows members can use (*continued*)

Parameter	Description
smc -updateconfig	<p>Checks whether the policy file on the management server is more recent than the policy file on the client.</p> <p>If the client policy file is out of date, updateconfig downloads the most recent policy file and replaces the existing policy file, which is serdef.dat.</p> <p>Returns 0</p>

You can run the parameters in [Table A-2](#) only if:

- The client runs Windows 2003/XP/Vista, or Windows Server 2008 and users are members of the Windows Administrators group.
- The client runs Windows 2003/XP and users are members of the Power Users group.

If the client runs Windows Vista and the User Account Control is enabled, the user automatically becomes a member of both the Administrators and Users group. To use the following parameters, users must be a member of the Administrators group only.

**Table A-2** Parameters that members of the Administrators group can use

Parameter	Description
smc -importconfig	<p>Replaces the contents of a policy file to the contents of the client's current policy file.</p> <p>This command does not replace the current policy file's contents. Therefore, you can deploy the most current policy file without having to remove out-of-date firewall rules, antivirus scans, security settings, and user interface settings.</p> <p>You must specify the path name and file name. For example, you can type the following command:</p> <pre>smc -importconfig C:\policy\OfficeRules.xml.</pre> <p>Returns 0, -1, -5, -6</p>
smc -exportconfig	<p>Exports the policy file on the client to an .xml file.</p> <p>You must specify the path name and file name. For example, you can type the following command:</p> <pre>smc -exportconfig C:\policy\OfficeRules.xml</pre> <p>Returns 0, -1, -5, -6</p>

**Table A-2** Parameters that members of the Administrators group can use  
*(continued)*

Parameter	Description
smc -importadvrule	<p>Replaces the imported firewall rules to the client's list of existing firewall rules.</p> <p>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. The client must run to import the policy file's contents.</p> <p>Imported firewall rules and client rules only apply to the client in client control or mixed control. The client ignores these rules in server control.</p> <p>To import firewall rules, you import a .sar file. For example, you can type the following command:</p> <pre>smc -importadvrule C:\config\AllowExplorerRule.sar</pre> <p>An entry is added to the System log after you import the rules.</p> <p>Returns 0, -1, -5, -6</p>
smc -exportadvrule	<p>Exports the client's firewall rules to a .sar file.</p> <p>Client rules only apply to the client in client control or mixed control. The client ignores these rules in server control.</p> <p>You must specify the path name and file name. For example, you can type the following command:</p> <pre>smc -exportadvrule C:\config\AllowExplorerRule.sar</pre> <p>Returns 0, -1, -5, -6</p>
smc -start	<p>Starts the Symantec Endpoint Protection or Symantec Network Access Control client service.</p> <p>Returns 0, -1</p>
smc -stop	<p>Stops the Symantec Endpoint Protection or Symantec Network Access Control client service and unloads it from memory.</p> <p>Returns 0, -1</p>

When you import policy files and firewall rules, note that the following rules apply:

- You cannot import policy files or firewall rule files directly from a mapped network drive.

- The client does not support UNC (universal naming convention) paths.

## Error codes

[Table A-3](#) displays the error codes that the `smc` command returns when the required parameters are invalid or missing.

**Table A-3** Smc error codes

Error code	Description
0	Command was successful.
-1	User is not in the Windows Administrators or Windows Power Users group. If the client runs Windows Vista, the user is not a member of the Windows Administrators group.
-2	Invalid parameter. You may have typed the parameter incorrectly, or you may have added an incorrect switch after the parameter.
-3	<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, policy file name (.xml) or firewall rules file name (.sar).

## Typing a parameter if the client is password-protected

You can password-protect the client computer for the following parameters:

- stop                   The client asks for a password before you or the user stops the client.
- importconfig        The client asks for a password before you can import the policy file.
- exportconfig         The client asks for a password before you can export the policy file.

See [“Password-protecting the client”](#) on page 109.

---

**Note:** The password is limited to 15 characters or less.

---

**To type a parameter if the client is password-protected**

- 1 On the client computer, on the taskbar, click **Start > Run**.
- 2 In the Run dialog box, type **cmd**
- 3 In the Windows MS-DOS prompt, type either one of the following:

```
smc -parameter -p password
```

```
smc -p password -parameter
```

Where:

*parameter* is `-stop`, `-importconfig`, or `-exportconfig`.

*password* is the password you specified in the console.

For example, you can type either:

```
smc -exportconfig c:\profile.xml -p password or
```

```
smc -p password -exportconfig c:\profile.xml
```

- 4 Close the command prompt.

# Index

## A

- Active Directory domain controller
  - automatic exclusions 367
- Active Directory server
  - importing user information from 55
- active directory servers 235
  - filter 235
- active response
  - setting up 452
- adapters. *See* network adapters
- add a group 56
- adding
  - an administrator 69
- administrator
  - about 68
  - adding 69
  - change password 74
  - editing properties 71
  - removing 74
  - renaming 73
  - tasks 69
- administrator-defined scans 411
  - See also* on-demand scans
  - See also* scheduled scans
- administrators
  - types of 68
- adware 361
- aggregation 278
- antispysware options
  - Host Integrity requirements 565
- Antivirus and Antispyware Policies
  - about 355
  - default policy 356
  - High Performance policy 356
  - High Security policy 357
  - legacy clients 357
  - locking settings 357
  - managing client interaction 376
  - scheduled scans 412
  - setting up log handling 375
  - setting Windows Security Center options 377
- Antivirus and Antispyware Policies (*continued*)
  - submissions options 387
  - working with 359
- Antivirus and Antispyware Protection
  - basics 352
  - locking and unlocking features 104
- antivirus options
  - Host Integrity requirements 564
- application and device control
  - logs 173, 203, 502
  - reports 149, 203
  - rules 499
- Application and Device Control Policies 46
  - creating 504
  - rules
    - disabling 512
    - priorities 511
  - structure 496
  - types of controls 496
  - working with 502
- Application Control
  - configuring 505
- application control rule set
  - modes 498, 513
  - setting priorities 511
- application triggers
  - firewall rules 428
- application-level control 497
- applications 473
  - See also* learned applications
  - adding to a rule 472
  - authorizing 524
  - defining 473
  - monitoring networked applications 477
  - options in Host Integrity requirements 566
  - restoring for Host Integrity 558
  - searching for 346, 473
- assistive technology
  - creating centralized exceptions for 533, 539, 542
- attacks
  - blocking 424, 452

- attacks (*continued*)
    - signatures 447
  - audit
    - log 174
    - report 150
  - authentication
    - certificate 253
    - peer-to-peer 445
  - Auto-Protect
    - advanced scanning and monitoring options 399
    - configuring 395
    - configuring notification options 404
    - configuring progress notifications 410
    - displaying results on infected computers 406
    - for file system
      - configuring 397
      - enabling 396
    - for Internet email 401
    - Lotus Notes 403
    - Microsoft Outlook 402
    - scans 363
    - security risk scanning and blocking 398
    - types of 396
  - automatic exclusions
    - about 365
    - for Active Directory domain controller 367
    - for Microsoft Exchange server 366
    - for Symantec products 367
- B**
- backup
    - database 261
    - embedded database from the Symantec Endpoint Protection Manager console 268
    - Microsoft SQL database from Symantec Endpoint Protection Manager console 264
    - Microsoft SQL database with MS SQL wizard 265
  - blank rules 436
  - blended threats 360
  - blocking
    - clients from groups 61
  - blocking attacking computers 452
  - bots 360
- C**
- cancel
    - Host Integrity remediation 559
  - centralized exceptions 531
    - See also* Centralized Exceptions Policies
    - assistive technology applications 539, 542
    - extensions 537
    - files 536
    - folders 536
    - for antivirus and antispyware scans 532
    - for detected processes 538
    - for proactive threat scans 488
    - for TruScan proactive threat scans 533, 537
    - forcing a TruScan detection 538
    - known security risks 535
    - risk events 541
    - Tamper Protection 533, 539
    - Tamper Protection events 542
    - TruScan proactive threat scan events 541
  - Centralized Exceptions Policies 531
    - See also* centralized exceptions
    - client interaction 534
    - client restrictions 540
    - configuring 534
    - creating exceptions from log events 540
    - exceptions for antivirus and antispyware scans 535
    - exceptions for TruScan proactive threat scans 537
    - working with 532
  - certificate
    - certificate and private key file (DER and PEM format) 254
    - digital 253
    - JKS keystore file 253
    - PKCS12 keystore file 254
    - server 253
    - update 254
  - CGI errors
    - database 284
  - class ID
    - about 515
  - ClassGuid 516
  - client 295
    - See also* replication
    - commands 583
    - Control Log 502
    - definition 53
    - deleting upgrade packages 84
    - determine the location of 53
    - offline 219
    - package replication 295

- client (*continued*)
  - password protection 109
  - rules 434
  - updates
    - Intelligent Updater 97
    - third-party distribution tools 97
  - user interface
    - access to 103
    - configuring 104–105, 108
- client computer
  - modes 54
- client computer mode
  - default 54
- client control 106
- client install packages
  - configuring 78
- client installation packages
  - about 77
  - adding 81
  - adding updates 82
  - collecting user information 79
  - configuring 78–79
  - exporting 80
- client types 53
- clients
  - search for 64
- collect user information 79
- commands
  - client 583
  - running from logs 186
- communication between a directory server and Symantec Endpoint Protection Manager
  - about 55
- communication settings
  - client and server 120
- compliance
  - logs 174, 204
  - reports 150, 204
- computer status
  - logs 175, 206
  - reports 151, 206
- computer-based mode 54
- computers
  - search for 64
- computers and users
  - about 54
- considerations
  - switching modes 60

- console
  - increasing timeout period 226
- control levels 105
- custom requirements
  - about 563
  - AND, OR keywords 572
  - comments 575
  - conditions 564
  - copying statements 576
  - deleting statements 576
  - ELSE statement 572, 575
  - functions 570
  - IF, THEN, ENDIF statement 572
  - NOT keyword 572
  - RETURN statement 571
  - writing 573

## D

- database
  - backup 261
    - automatic 269
  - backups 263
  - CGI errors 284
  - changing timeout parameters 284
  - edit
    - description 271
    - name 271
  - embedded
    - naming convention 260
  - errors 284
  - maintaining 282–283
  - management 259
  - Management Server Configuration Wizard 260
  - Microsoft SQL
    - naming conventions 260
  - MS SQL
    - bcp.exe file 273
  - reconfiguration 262
  - reconfiguring
    - embedded 274
    - MS SQL 272
  - restoring 261
    - procedure 270
  - scheduling automatic backup 269
  - size 261
  - Symantec Database Backup and Restore
    - utility 260
  - terminated process errors 284
- default policy 304

- definitions files
  - configuring actions for new definitions 393
  - displaying out-of-date or missing 379
  - scanning after updating 370
- delete
  - group 57
- delete users and computers
  - about 62
- DER and PEM format 254
- detection rates
  - sending information to Symantec 388
- device ID
  - about 515
  - as device control 501
- device-level control
  - application and device control 501
  - reports 149
- DHCP traffic 443
- dialers 361
- directory servers
  - active 235
  - adding 236
  - LDAP 235
  - synchronizing 237
- displaying user and computer properties 63
- DNS traffic 443
- domains
  - about 51
  - adding 55
  - administering 56

**E**

- ELSE statements 575
- email messages 401, 408
  - See also* infected email messages
  - See also* Internet Email Auto-Protect
  - for firewall rules 476
- encryption 253
- Enforcers
  - restoring Host Integrity 558
- event logs 180
  - past 24-hours filter 143, 183
- events
  - about 125
  - aggregation 278–279
  - database maintenance
    - options 283
- exceptions 451, 531
  - See also* centralized exceptions

- exceptions (*continued*)
  - IPS signatures 451
- excluded hosts 453
- exclusions. *See* centralized exceptions
  - created automatically 365
- exporting
  - client installation packages 80
  - firewall rules 440
  - management server list 118
  - policies 333
- extensions
  - scanning selected 382
- external logging 189

**F**

- failover 112
- false positives 449, 484
  - minimizing 454
- Favorite Reports
  - Symantec Endpoint Protection
    - customizing 135
- file fingerprints 520
- File System Auto-Protect. *See* Auto-Protect
- files
  - excluding from scanning 374
  - options in Host Integrity requirements 566
  - restoring for Host Integrity 558
  - sharing 469
- filter
  - settings 65
- filters 182
- firewall
  - about 424–425
  - Host Integrity requirements 565
  - notifications 475
  - traffic settings 444
- firewall logs and reports. *See* Network Threat Protection
- Firewall Policies
  - about 425–426
- Firewall Rule Wizard 438
- firewall rules
  - about 427, 434
  - actions 428
  - adding
    - using blank rule 436
    - using wizard 438
  - applications 428
    - adding 472



- firewall rules (*continued*)
  - changing the order 442
  - client 434
  - conditions 427
  - copying 442
  - deleting 441
  - disabling 443
  - editing 441
  - elements of 427
  - email messages 476
  - enabling 443
  - exporting 440
  - host groups
    - adding 465
    - creating 464
    - editing and deleting 465
  - hosts 429
  - importing 440
    - limitations 586
  - inheriting 433, 439
  - list 432
  - network adapter triggers 431
  - network adapters
    - adding 470–471
    - editing and deleting 472
  - network service triggers 430
  - network services
    - adding 466, 468
    - editing and deleting 467
  - pastings 442
  - processing order 432
    - changing 442
  - schedules
    - adding 474
  - server 434
  - triggers 427
- folders
  - scanning selected 382
- FTP proxy server 245
- functions
  - Download a file 577
  - Log message 578
  - Run a program 578
  - Run a script 579
  - Set Timestamp 580
  - Show message dialog 576
  - Wait 581

## G

- Global
  - group 52
- group
  - add 56
  - adding a computer 59
  - blocking 61
  - delete 57
  - move 57
  - rename 57
  - root 52
  - structure 51
  - Temporary 52
- group hierarchy
  - sample 52
- group inheritance. *See* inheritance
- group properties
  - viewing 58
- Group Update Provider
  - configuring in a Settings Policy 95
  - ports and communications 95
- groups
  - about 50–51
  - assigning management server list 114
  - search for 64
  - specifying a management server list 112
- GUID
  - as device control 501

## H

- hack tools 361
- hardware devices
  - setting up 515
- Home page
  - Symantec Endpoint Protection
    - about 128
    - customizing 135
    - Security Response links 136
    - using 129
  - Symantec Network Access Control
    - about 138
    - using 138
- host groups
  - adding to a rule 465
  - creating 464
  - deleting 465
  - editing 465
- Host Integrity
  - about 46

- Host Integrity checks
    - forcing a pass 557
    - logging details 555
    - notifications 555
    - policy change 554
    - settings 554
    - verbose logging 555
  - Host Integrity Policies
    - about 550
    - creating 550
      - shared 550
    - custom requirements
      - about 563
      - antispyware conditions 565
      - antivirus conditions 564
      - download a file 577
      - file options 566
      - firewall conditions 565
      - log message 578
      - message box 576
      - operating system conditions 568
      - registry options 568
      - run a program 578
      - run a script 579
      - set timestamp 580
      - wait option 581
      - writing 573
    - requirements
      - adding 552
      - defining 549
      - deleting 552
      - editing 552
      - enabling and disabling 553
      - example 546
      - passing even when condition not met 557
      - planning 548
      - sequencing 553
      - templates 553
      - types 550
    - restoring Host Integrity 557–559
      - Enforcer settings 558
      - postponing 560
    - self enforcement 545
    - working with 548
  - host triggers
    - firewall rules 429
  - hosts
    - adding to a rule 465
    - excluding from intrusion prevention 453
  - hosts (*continued*)
    - local and remote 429–430
    - source and destination 429
  - HTTP protocol 113
  - HTTP proxy server 245
  - HTTPS protocol 113
- I**
- ICMP traffic 435
  - icons
    - padlock 104
  - IF condition statement 576
  - IF THEN statements 574
  - import groups
    - from LDAP server 55
  - importing
    - firewall rules 440
      - limitations 586
    - Host Integrity Policy requirements
      - templates and 553
    - organizational units 241
    - policies 333
    - policy files
      - limitations 586
    - user information from an LDAP server 237
    - user information from LDAP directory server
      - search 240
  - infected computers
    - displaying Auto-Protect results on 406
  - infected email messages
    - adding warning to 406
    - notifying others 408
    - notifying senders 407
  - inheritance
    - enabling 310
    - firewall rules 433, 439
    - location
      - override 310
    - policy 309
      - override 310
  - inherited policy
    - moving a group with 58
  - inspection. *See* stateful inspection
  - Internet bots 360
  - Internet Email Auto-Protect 401
  - intrusion prevention
    - about 424, 447
    - blocking attacking computers 452
    - configuring 449

intrusion prevention (*continued*)  
 disabling on specified computers 453  
 enabling 450  
 notifications 476

IPS engines 447  
 packet-based 449  
 stream-based 448

IPS exceptions 451

IPS signatures  
 custom  
 about 448  
 assigning libraries to a group 456  
 building a library 454  
 changing the order 457  
 copying and pasting 457  
 creating 454  
 libraries 454, 456  
 variables 458

Symantec  
 about 448  
 changing the behavior of 451  
 exceptions 451

IPv4 466

IPv6 466

## J

JKS keystore file 253

joke programs 361

## K

Knowledge Base 354

## L

LDAP directory server  
 importing user information to management  
 server 237

LDAP directory servers 235

filter 235

importing

organizational units 241

user information from a LDAP directory  
 server search 240

searching for users 238

LDAP protocol 237

LDAP server

import groups from 55

importing user information from 55

learned applications 473

*See also* applications

about 343

enabling 344–345

list 473

saving search results 347

searching for 346

legacy clients

Antivirus and Antispyware Policies for 357

libraries. *See* IPS signatures

limited administrators

about 68

LiveUpdate

advanced distribution options 96

changing Content Policies applied to groups 95

configuring

a Content Policy 93

a Group Update Provider 95

a Settings Policy 92

a site to download updates 89

LiveUpdate Administrator 89

MSI and MSP files 89

network distribution architectures 86

policies

about 92

configuring 92–93

signatures and definitions 89

third-party distribution options 87

types of updates 89

updating definitions and content 85

using third-party distribution tools instead of 97

using with replication 89

load balancing 112

location inheritance 309

locked and unlocked settings

client 104

locks

in Antivirus and Antispyware Policies 357

padlock icons 104

logs 171, 203

about 125

application and device control 173, 203

audit 174

clearing from database 277

client

configuring size 279

Client Control Log 502

compliance 174, 204

computer status 175, 206

logs *(continued)*

- database errors 180
- database maintenance
  - options 283
- deleting configuration settings 183
- event details 181
- exporting data 189
- filtering 182
- managing 282
- Network Threat Protection 176, 208
- Notifications 177
- past 24-hours filter 183
- refreshing 180
- remote access 181
- replicating 181
- Risk 176, 211
  - deleting files from the Quarantine 186
- running commands from 186
- saving filter configurations 182
- Scan 176, 213
- server
  - configuring size 277
- storage 275
- System 177, 213
- TruScan Proactive Threat Scan 176, 210
- types 172
- viewing 180
- viewing remotely 181

**M**

- managed settings
  - configuring on client 103
  - locking and unlocking 104
- management server
  - editing 116
- Management Server Configuration Wizard 260
- management server list
  - about 112
  - adding 113
  - assigning to group and location 114
  - copying 118
  - default list 112
  - deleting 119
  - displaying assigned groups and locations 115
  - editing 116
  - exporting and importing 118
  - pasting 118
  - replacing 117
  - server priority 117

management server list *(continued)*

- specifying for a group 112
- managing administrators
  - about 69
- manual scans. *See* on-demand scans
- Microsoft Exchange server
  - automatic exclusions 366
- Microsoft SQL
  - managing database 259
- mixed control 106
  - about 107
  - configuring Network Threat Protection settings 463
- modes 513
  - client computer 54
- move
  - group 57
- moving users and computers
  - about 62
- MSI files 89
- MSP files 89

**N**

- network adapters
  - adding to a rule 471
  - adding to default list 470
  - editing and deleting 472
  - triggers 431
- network application monitoring 477
- network architecture options
  - for LiveUpdate and content distribution 86
  - for third-party management of updates 87
- network services
  - adding to a rule 468
  - adding to default list 466
  - deleting 467
  - editing 467
  - triggers 430
- Network Threat Protection
  - configuring for mixed control 463
  - creating notifications 475
  - disabling 462
  - enabling 462
  - logs 176, 208
  - overview 424
  - reports 153, 208
- non-shared policy. *See* policy
- notification messages
  - for antivirus and antispyware scans 385

notifications

- Auto-Protect options 404
- log 177
- Network Threat Protection 475
- TruScan proactive threat scan 494

## O

- offline clients 219
- on-demand scans
  - advanced options 419
  - configuring 415
  - running 416
  - scan progress options 418
- operating system conditions
  - Host Integrity requirements 568
- organizational structure
  - about 50
- organizational unit
  - importing 54
- organizational units
  - importing 241
  - synchronizing 242
- Other risk category 361

## P

- padlock icons 104
- parent group. *See* inheritance
- password
  - third party 230
- password change
  - administrator 74
- password protection
  - changing password 376
  - client 109
  - parameters 587
  - scanning mapped drives 376
- PC-cillin 428
- peer-to-peer authentication 445
- PKCS12 keystore file 254
- policy
  - about 303, 322
  - add non-shared
    - Clients page 324, 326
    - from exported 327
  - add shared
    - from existing shared 326
    - Policy page 323
  - assign shared 329

policy (*continued*)

- default 304
- delete non-shared 332
- delete shared 331
- edit non-shared
  - Clients page 328
- edit shared
  - Clients page 328
  - Policies page 327
- example 308
- export shared
  - Policies page 333
- import 333
- importing policy files 586
- inheritance 309
- LiveUpdate 92
- non-shared 305
- shared 305
- withdraw 330
- preferences
  - reporting 140
- print sharing 469
- Proactive Threat Protection 482
  - about 46
  - reports 210
- proactive threat scans. *See* TruScan proactive threat scans
- Production mode 498, 513
- properties
  - group 58
- protocol
  - LDAP 237
- protocols
  - adding 466
  - adding to a rule 468
  - editing and deleting 467
  - HTTP 113
  - HTTPS 113, 253
- proxy server
  - FTP 245
  - HTTP 245

## Q

- Quarantine
  - about 358
  - clean-up options 391
  - deleting files 186
  - forwarding items to Central Quarantine Server 392

Quarantine (*continued*)

- local directory 390
- managing items 358
- sending items to Symantec 393
- settings 390

## quick reports

- basic filter settings 165
- creating 165

**R**

## reconfiguration

- database 262
- embedded database 274
- Microsoft SQL database 272

## registry options

- Host Integrity requirements 568

## remediation

- Host Integrity 557
  - applications 558
  - files 558
  - postponing 560
  - wait time 559

## remote access programs 362

## remote consoles

- granting access 231

## removing

- an administrator 74

## rename

- group 57

## renaming

- an administrator 73

## replication

- adding replication partner 292
- client package 295
- communication settings 290
- disconnecting replication partner 293
- example 290
- frequency 295
- illustrated example 289
- LiveUpdate and 89
- logs 296
- merging of data 291
- on demand scheduling 294
- overview 287
- setup
  - initial 292
  - post-installation 292

## reporting

- basics 122

reporting (*continued*)

- Home page preferences 140
- important points 161
- logs 171
- Symantec Endpoint Protection
  - Home page 128
- Symantec Network Access Control
  - Home page 138

## reports 168

- See also* scheduled reports
- application and device control 203
- application control 149
- audit 150, 203
- compliance 150, 204
- computer status 151, 206
- configuring filters 124
- deleting configuration settings 166
- device control 149
- Network Threat Protection 153, 208
- overview 123
- past 24-hours filter 143
- printing 167
- Proactive Threat Protection 210
- quick 148
- Risk 155, 211
  - saving 167
- saving configuration settings 166
- Scan 158, 213
- System 159, 213
- types 123

## restoration

- database 261

## risk 359

- See also* security risks
- detection 359
- eliminating 216
- logs 176, 211
  - deleting files from the Quarantine 186
- reports 155, 211

## Risk Tracer 399

- blocking IP addresses 400

## rootkits 359

## RSA SecurID

- authentication prerequisites 73

## RSA server

- configuring SecurID authentication 250
- using with Symantec Endpoint Protection Manager 249

rule priorities

Application and Device Control Policies 511

rules. *See* firewall rules

## S

Scan

logs 176, 213

reports 158, 213

scans 368

*See also* scheduled scans

about 363

advanced options for administrator-defined scans 419

antivirus and antispysware 381

centralized exceptions for 532

assigning actions 374

Auto-Protect 363

displaying warning message on client 385

excluding files from scanning 374

paused 418

recommended file extensions 373

running on demand 416

scan progress options 418

selecting files and folders to scan 370

snoozed 418

stopped 418

schedule

automatic database backup 269

on-demand embedded database backup 268

on-demand Microsoft SQL database backup 264

on-demand Microsoft SQL database backup with Database Maintenance wizard 265

scheduled reports 168

*See also* reports

about 168

creating 169

deleting 170

modifying 169

scheduled scans 368

*See also* scans

about 368

adding to a policy 412

advanced options 419

editing, deleting, or disabling 414

options when missed 413

saving as template 412

scan progress options 418

schedules

adding to a rule 474

screen reader

application blocked by Tamper Protection 533

search

clients 64

search for

groups, users, and computers 64

Search for Applications

custom requirements 567

SecurID authentication

configuring on the management server 250

specifying for an administrator 251

Security Response Web site

Symantec Endpoint Protection

accessing from Home page 136

security risks 359

*See also* risk

about actions for 374

actions 357

configuring actions for 384

ignoring during scanning 383

process continues to download 365

security topology

about 50

sending threat information to Symantec 387

server

adding directory server 236

directory 235

FTP proxy 245

HTTP proxy 245

logs 277

management 229

rules 434

server control 105

server settings

exporting and importing 233

services

adding 466

adding to a rule 468

editing and deleting 467

set up

hardware devices 515

settings

firewall 426, 444

Network Threat Protection 463

share files and printers 469

shared policy. *See* policy

signatures. *See* IPS signatures

Smart traffic filtering 443

- smc command
    - about 583
  - spyware 362
  - stateful inspection
    - about 435
    - creating rules for traffic 435
  - stealth settings 444
  - submissions 388
    - configuring options for 389
    - sending information to Symantec 387
    - sending items to Symantec 393
    - sending to Central Quarantine Server 392
  - suspicious files 357
  - switching client modes
    - about 60
  - Symantec Database Backup and Restore utility 260
  - Symantec Endpoint Protection Manager
    - automatic service start 230
    - deleting
      - multiple installations 232
  - Symantec products
    - automatic exclusions 367
  - Symantec Security Response 354
    - submissions 388
  - synchronizing
    - directory servers 237
    - organizational units 242
    - user information 55
  - System
    - logs 177, 213
    - reports 159, 213
  - system administrator
    - default 69
    - tasks 69
  - system administrators
    - about 68
  - system lockdown
    - enabling 526
- T**
- Tamper Protection
    - centralized exceptions 533, 539
    - locking and unlocking features 104
    - management 297
    - messages 298
  - TCP traffic 435
  - templates
    - for scheduled scans 412
  - Temporary group 52
  - terminated process errors
    - database 284
  - Test mode 498, 513
  - third party
    - password 230
  - third-party content distribution
    - about 97
    - enabling with a LiveUpdate Policy 98
    - registry key requirement for unmanaged 101
    - to managed clients 98
    - using with unmanaged clients 101
  - threats 210, 424
    - See also* Network Threat Protection
    - See also* Proactive Threat Protection
    - blended 360
  - timeout parameters
    - database 284
  - trackware 362
  - traffic
    - enabling Smart traffic 443
    - settings 444
  - Trend Micro PC-cillin 428
  - triggers
    - application 428
    - firewall rules 427
    - host 429
    - network adapter 431
    - network service 430
  - Trojan horses 360, 477
  - TruScan
    - sending information to Symantec 387
  - TruScan Proactive Threat Scan
    - log 210
    - logs 176
  - TruScan proactive threat scans
    - actions 491
    - centralized exceptions 488, 533, 537
    - commercial applications 492
    - defaults 482
    - detecting processes 483
    - false positives 484
    - forced detection 489
    - forcing a detection 538
    - frequency 493
    - ignoring processes 487
    - managing detections 490
    - notifications 494
    - processes 491
    - Quarantine 488



TruScan proactive threat scans *(continued)*  
 sensitivity level 491  
 Symantec defaults 482  
 types of clients 53

## U

UDP traffic 436  
 unmanaged clients  
   distributing updates with third-party tools 101  
 upgrading clients 81  
 upgrading clients in one or more groups 83  
 URL  
   appearing in error notifications 380  
   specifying browser home page 381  
 user and computer properties  
   displaying 63  
 user control levels 105  
 user information  
   collect 79  
 user interface  
   about 103  
   configuring 104–105, 108  
 user-based mode 54  
 users  
   add to domain 58  
   search for 64  
 users and computers  
   about 54  
   filtering 65

## V

variables in signatures 458  
 virus outbreak plan 352  
 viruses 359–360  
   about actions for 374  
   actions 357  
   configuring actions for 384

## W

wait options  
   Host Integrity remediation 559  
 warning message  
   adding to infected email message 407  
   displaying on infected computer 385  
   example 385  
 Windows GUID  
   class ID 516

Windows Security Center 377  
   alerts 378  
   disabling 377  
   out-of-date time for definitions 379  
 WINS traffic 443  
 withdrawing  
   policy 330  
 worms 360

## X

XML  
   server settings 233

## Z

zero-day attacks 482