Symantec™ Protection Engine for Network Attached Storage 7.9 Implementation Guide
Symantec™ Protection Engine for Network Attached Storage 7.9 Implementation Guide

Legal Notice

Copyright © 2017 Symantec Corporation. All rights reserved.

Symantec, the Symantec Logo, the Checkmark Logo and 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 Notice document for this Symantec product that may be available at http://www.symantec.com/about/profile/policies/eulas/, the Third Party Legal Notice Appendix to this Documentation or TPIP ReadMe File accompanying this Symantec product for more information on the Third Party Programs.

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

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

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

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

Symantec’s support offerings include the following:

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

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

support.symantec.com

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

Contacting Technical Support

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

support.symantec.com

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

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

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

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

www.symantec.com/business/support/

Customer service
Customer service information is available at the following URL:

www.symantec.com/business/support/

Customer Service is available to assist with non-technical questions, such as the following types of issues:
- Questions regarding product licensing or serialization
- Product registration updates, such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade assurance and support contracts
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs, DVDs, or manuals
Support agreement resources

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

- Asia-Pacific and Japan: customercare_apj@symantec.com
- Europe, Middle-East, and Africa: semea@symantec.com
- North America and Latin America: supportsolutions@symantec.com
## Contents

Technical Support ........................................................................................................... 4

Chapter 1  Introducing Symantec™ Protection Engine for Network Attached Storage ........................................... 17

- About Symantec™ Protection Engine for Network Attached Storage ........................................ 17
- What's new in Symantec Protection Engine ................................................................................ 18
- Components of Symantec Protection Engine ........................................................................ 19
- How Symantec Protection Engine works .................................................................................. 22
  - About automatic load balancing ............................................................................................ 22
  - About supported protocols for Symantec Protection Engine .............................................. 23
- What you can do with Symantec Protection Engine .............................................................. 24
- Where to get more information ............................................................................................. 28

Chapter 2  Installing Symantec Protection Engine ............................................................ 29

- Before you install Symantec Protection Engine ...................................................................... 29
- System requirements ............................................................................................................. 30
  - System requirements to install Symantec Protection Engine on Windows ........................... 31
  - System requirements to install Symantec Protection Engine on Linux .............................. 32
- About installing Symantec Protection Engine ........................................................................ 35
  - About authentication modes in Symantec Protection Engine ........................................... 36
  - Installing Symantec Protection Engine on Windows .......................................................... 37
  - Upgrading Symantec Protection Engine on Windows ......................................................... 43
  - Installing Symantec Protection Engine on Linux ............................................................... 53
  - Upgrading Symantec Protection Engine on Linux ............................................................. 56
- Symantec Protection Engine post-installation tasks ........................................................... 61
  - Verifying, stopping, and restarting the Symantec Protection Engine daemon on Linux ........ 61
  - Verifying, stopping, and restarting the Symantec Protection Engine service on Windows .... 62
  - Clearing the Java cache ....................................................................................................... 64
  - About adding or changing authorized group name to access the Symantec Protection Engine console .......................................................... 64
Chapter 3  Activating licenses ......................................................... 88
  About licensing ............................................................................ 88
  About license activation ............................................................... 90
    If you do not have a serial number ........................................... 90
    Obtaining a license file .......................................................... 91
    Installing the license file ....................................................... 92
  About removing license files ..................................................... 93
  Checking the license status ....................................................... 93

Chapter 4  Configuring scanning services for client applications ................. 94
  About the communication protocols .......................................... 94
  Supported services by protocol .................................................. 95
  About working with ICAP ........................................................... 97
    Configuring ICAP options ....................................................... 98
  About working with the RPC protocol ..................................... 100
    About RPC configuration options ......................................... 101
    Configuring Symantec Protection Engine to use the RPC protocol ......................................................... 102
    Adding and removing RPC clients ......................................... 103
    Configuring the RPC connection options ................................ 104
    Notifying a file server when definitions are updated ............... 105
    Configuring the antivirus scan policy ..................................... 106
    Logging to the RPC client logging subsystem ......................... 107
    User identification and notification when a risk is found .......... 108
    Editing the service startup properties .................................... 108
Chapter 5 Protecting against risks .......................................................... 110

About scanning for risks ..................................................................... 110

About threat categorization and risk ratings .................................... 111

How Symantec Protection Engine detects risks .............................. 112

Enabling threat detection in Symantec Protection Engine ............... 114

Ways to test threat detection capabilities ....................................... 116

Enabling nonviral threat detection in Symantec Protection Engine .......... 117

Enabling advanced heuristic scanning in Symantec Protection Engine .......................................................... 118

About quarantining files in Symantec Protection Engine .................. 119

Configuring the quarantine in Symantec Protection Engine ............ 120

About preventing potential threats in Symantec Protection Engine .................. 121

Configuring file name filtering in Symantec Protection Engine .......... 122

Configuring true type file filtering in Symantec Protection Engine .......... 124

Configuring file size filtering in Symantec Protection Engine .......... 124

Configuring subject line content filtering in Symantec Protection Engine .......................................................... 126

Configuring message origin filtering in Symantec Protection Engine .......................................................... 128

About MS Office files in Symantec Protection Engine ..................... 129

About container files in Symantec Protection Engine ..................... 130

Configuring Symantec Protection Engine to handle partial container files .......................................................... 131

About unscannable files in Symantec Protection Engine .................. 132

Customizing notifications in Symantec Protection Engine ................. 135

Notifying RPC-client users that a threat was found ......................... 138

About Symantec Insight™ .............................................................. 139

How does Symantec Protection Engine use Symantec Insight™ ........ 139

About Symantec Insight™ result parameters ................................... 140

Enabling Symantec Insight™ policy ............................................. 141

Configuring the Symantec Insight™ aggression level ...................... 142

Excluding files from Insight scanning based on file size .................. 142

Excluding files from Insight scanning based on SHA256 ................. 143

About advanced machine learning ................................................. 144
Chapter 6  Modifying and tuning the performance of Symantec Protection Engine .......................................................... 145
  How to monitor Symantec Protection Engine performance ............. 145
  Monitoring scanning requests ...................................................... 146
  Monitoring Symantec Protection Engine resources ...................... 149
  Ways to improve Symantec Protection Engine performance ........... 154
  Deployment considerations and recommendations ...................... 154
  Enhance performance by limiting scanning .................................. 156
  Configuration settings that can conserve and enhance performance .......................................................... 163
  About telemetry data ................................................................ 166

Chapter 7  Filtering URLs ................................................................. 167
  About filtering URLs ................................................................ 167
  About categories .................................................................... 168
  How to filter a URL ................................................................... 182
  About the filtering modes ......................................................... 182
  Denying access to URLs in URL categories ............................... 184
  Managing local categories ....................................................... 185
  Overriding a URL categorization .............................................. 189
  Customizing the access denied message ................................... 190
  About URL Reputation ................................................................. 191
  Configuring URL Reputation .................................................... 191

Chapter 8  Android Application (APK) Reputation .......................... 193
  About Android Application (APK) Reputation ........................... 193
  Configuring the APK Reputation ................................................ 194

Chapter 9  Traffic monitor mode in Symantec Protection Engine ....... 196
  About traffic monitor mode in Symantec Protection Engine .......... 196
  Functional changes in Symantec Protection Engine .................... 197
  About traffic statistics summary collection: ................................. 197
  About traffic statistics collection .............................................. 198
  Configuring Symantec Protection Engine to function in Traffic monitor mode .......................................................... 199
Chapter 10  Logging data, issuing alerts, and generating reports ................................................................. 200
  About logging data ................................................................................................................................. 200
  Logging destinations ............................................................................................................................... 200
  Logging levels and events ....................................................................................................................... 202
  Specifying the log bind address ........................................................................................................... 205

  About configuring local logging ............................................................................................................ 207
  Specifying the local logging level .......................................................................................................... 207
  Changing the directory where log files are located .............................................................................. 208
  Maintaining log files on a shared resource in Windows ......................................................................... 209
  Changing the length of time that log files are maintained ................................................................... 210
  Enabling statistics reporting in Symantec Protection Engine .............................................................. 211

  Configuring logging to the Windows Application Event Log .............................................................. 212
  Configuring logging to the Linux Syslog ............................................................................................... 213

  About configuring alerts ....................................................................................................................... 213
  Activating SMTP alerts ......................................................................................................................... 214
  Activating SNMP alerts ......................................................................................................................... 215
  Configuring outbreak alerts ................................................................................................................. 216

  About reports ......................................................................................................................................... 218
  Viewing the local log data ...................................................................................................................... 219
  Exporting local log data to a file ........................................................................................................... 220
  Viewing statistics log data ..................................................................................................................... 221
  About summary report on Symantec Protection Engine home page ..................................................... 222

Chapter 11  Keeping your product up to date .............................................................................................. 226
  About content updates ........................................................................................................................... 226
  About definition updates ......................................................................................................................... 226
  About updating your protection ............................................................................................................ 227

  About LiveUpdate .................................................................................................................................. 229
  Configuring LiveUpdate to occur automatically .................................................................................. 230
  Performing LiveUpdate on demand ....................................................................................................... 231
  About scheduling LiveUpdate using the command line ...................................................................... 231
  About setting up your own LiveUpdate server .................................................................................... 232
  About editing the LiveUpdate XML file ............................................................................................... 232
  About LiveUpdate logging ..................................................................................................................... 233

  About Intelligent Update ....................................................................................................................... 237
  Enabling definition updates through Intelligent Update ....................................................................... 240
  Updating definitions using Intelligent Update ....................................................................................... 241
  Disabling definition updates through Intelligent Update ....................................................................... 242

  About Rapid Release ............................................................................................................................. 243
  Configuring Rapid Release updates to occur automatically ................................................................. 244
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Performing Rapid Release updates on demand</td>
<td>245</td>
</tr>
<tr>
<td>Rolling back definitions</td>
<td>245</td>
</tr>
<tr>
<td>Chapter 12 Working with the Core server only mode</td>
<td>247</td>
</tr>
<tr>
<td>About the Core server only mode</td>
<td>249</td>
</tr>
<tr>
<td>About XMLModifier tool</td>
<td>250</td>
</tr>
<tr>
<td>XMLModifier options</td>
<td>251</td>
</tr>
<tr>
<td>Accessing the XML modifier command-line tool</td>
<td>255</td>
</tr>
<tr>
<td>Configuring ICAP options in the Core server only mode</td>
<td>255</td>
</tr>
<tr>
<td>Configuring Symantec Protection Engine to use the RPC protocol in the Core server only mode</td>
<td>257</td>
</tr>
<tr>
<td>Adding and removing RPC clients in the Core server only mode</td>
<td>258</td>
</tr>
<tr>
<td>Configuring the RPC connection options in the Core server only mode</td>
<td>259</td>
</tr>
<tr>
<td>Notifying a file server when definitions are updated in Core server only mode</td>
<td>260</td>
</tr>
<tr>
<td>Configuring the antivirus scan policy in the Core server only mode</td>
<td>261</td>
</tr>
<tr>
<td>Enabling threat detection in the Core server only mode</td>
<td>262</td>
</tr>
<tr>
<td>Enabling nonviral threat detection in the Core server only mode</td>
<td>265</td>
</tr>
<tr>
<td>Enabling advanced heuristic scanning in the Core server only mode</td>
<td>266</td>
</tr>
<tr>
<td>Configuring APK Reputation in the Core server only mode</td>
<td>267</td>
</tr>
<tr>
<td>Enabling advanced machine learning in the Core server only mode</td>
<td>268</td>
</tr>
<tr>
<td>Configuring the quarantine server in the Core server only mode</td>
<td>269</td>
</tr>
<tr>
<td>Configuring file name filtering in the Core server only mode</td>
<td>270</td>
</tr>
<tr>
<td>Configuring file size filtering in the Core server only mode</td>
<td>273</td>
</tr>
<tr>
<td>Configuring true type file filtering in the Core server only mode</td>
<td>275</td>
</tr>
<tr>
<td>Configuring subject line content filtering in the Core server only mode</td>
<td>276</td>
</tr>
<tr>
<td>Configuring message origin filtering in the Core server only mode</td>
<td>278</td>
</tr>
<tr>
<td>Configuring Symantec Protection Engine to handle partial container files in the Core server only mode</td>
<td>279</td>
</tr>
<tr>
<td>Configuring Symantec Protection Engine to handle malformed container files in the Core server only mode</td>
<td>280</td>
</tr>
<tr>
<td>Configuring Symantec Protection Engine to handle encrypted container files in the Core server only mode</td>
<td>282</td>
</tr>
<tr>
<td>Customizing notifications in the Core server only mode</td>
<td>284</td>
</tr>
<tr>
<td>Notifying RPC client users that a threat was found in the Core server only mode</td>
<td>289</td>
</tr>
<tr>
<td>Enabling Symantec Insight™ in the Core server only mode</td>
<td>290</td>
</tr>
</tbody>
</table>
Configuring the Symantec Insight™ aggression level in the Core server only mode ................................................................. 292
Excluding files from Insight scanning based on file size in the Core server only mode ................................................................. 292
Excluding files from Insight scanning based on SHA256 in the Core server only mode ............................................................... 293
Excluding files from Insight scanning based on source IP address in the Core server only mode ................................................. 294
Excluding files from Insight scanning based on source URL in the Core server only mode ....................................................... 294
Monitoring scanning requests in the Core server only mode .......... 295
Enabling resource consumption logging in the Core server only mode ......................................................................................... 298
Specifying the maximum file or message size to scan in the Core server only mode ................................................................. 299
Setting container file limits in the Core server only mode ................. 300
Enabling URL filtering in the Core server only mode ....................... 303
Denying access to URLs in URL categories in the Core server only mode ................................................................. 304
Customizing the access denied message in the Core server only mode ....................................................................................... 304
Specifying the log bind address in the Core server only mode .......... 305
Specifying the local logging level in the Core server only mode ....... 306
Changing the directory where log files are located in the Core server only mode ................................................................. 307
Maintaining log files on a shared resource in Windows in the Core server only mode ................................................................. 308
Changing the number of log file to be maintained in the Core server only mode ................................................................. 309
Enabling statistics reporting in the Core server only mode ............... 310
Configuring logging to the Windows Application Event Log in the Core server only mode ............................................................. 311
Configuring logging to the Linux Syslog in the Core server only mode ....................................................................................... 312
Activating SMTP alerts in the Core server only mode ....................... 312
Activating SNMP alerts in the Core server only mode .................... 314
Configuring outbreak alerts in the Core server only mode ............... 316
Configuring LiveUpdate to occur automatically in the Core server only mode ................................................................. 319
Configuring Rapid Release updates to occur automatically in the Core server only mode ............................................................. 320
Configuring Rapid Release to download definitions from HTTP Server ....................................................................................... 321
Appendix A
Performing a silent installation .................................................. 325

About silent installation and upgrade ............................................. 325
Implementing a silent installation in Linux ........................................ 326
Creating the response file ......................................................... 326
About initiating a silent installation using the response file .......... 331
About implementing a silent installation for Windows ................. 331
Initiating a silent installation on Windows ................................... 335
Generating an encrypted password .............................................. 336

Appendix B
Using the Symantec Protection Engine command-line scanner .......... 337

About the Symantec Protection Engine command-line scanner .......... 337
Setting up a computer to submit files to Symantec Protection Engine
for scanning ........................................................................ 338
C-based command-line scanner syntax and usage ............................ 339
Supported command-line options for C-based command-line
scanner .............................................................................. 341
About specifying the Symantec Protection Engine IP address and
port for C-based command-line scanner .................................. 346
About specifying the antivirus scanning mode for C-based
command-line scanner ....................................................... 347
About obtaining scan results for C-based command-line
scanner .............................................................................. 347
About requesting recursive scanning ........................................... 350
About disposing of infected files when an error occurs .................. 351
Excluding files from scanning ................................................. 351
Redirecting console output to a log file ....................................... 352
About scanning files in Symantec Protection Engine using different
services/APIs ....................................................................... 353
About using Insight command options with C-based command-line
scanner .............................................................................. 354
Java based command-line scanner syntax and usage ....................... 355
Supported command-line options for Java based command-line
scanner ............................................................................... 356
About specifying the Symantec Protection Engine IP address and
port for Java based command-line scanner ................................ 359
About specifying the antivirus scanning mode for Java based
command-line scanner ......................................................... 360
About obtaining scan results for Java based command-line
scanner .............................................................................. 361
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>About scanning files in Symantec Protection Engine using different</td>
<td>362</td>
</tr>
<tr>
<td>services/ APIs with Java based command-line scanner</td>
<td></td>
</tr>
<tr>
<td>About using Insight command options with Java based</td>
<td>362</td>
</tr>
<tr>
<td>command-line scanner</td>
<td></td>
</tr>
<tr>
<td>Appendix C</td>
<td>365</td>
</tr>
<tr>
<td>About editing configuration data</td>
<td></td>
</tr>
<tr>
<td>About editing the Symantec Protection Engine configuration files</td>
<td>365</td>
</tr>
<tr>
<td>About configuration options</td>
<td>366</td>
</tr>
<tr>
<td>Configure the ICAP response</td>
<td>368</td>
</tr>
<tr>
<td>Configure the ICAP preview option</td>
<td>369</td>
</tr>
<tr>
<td>Control the dynamic thread pool</td>
<td>369</td>
</tr>
<tr>
<td>Disable the ICAP threshold client notification</td>
<td>372</td>
</tr>
<tr>
<td>Configure the number of LiveUpdate retries</td>
<td>372</td>
</tr>
<tr>
<td>Change the LiveUpdate base time</td>
<td>373</td>
</tr>
<tr>
<td>Configure the LiveUpdate server details</td>
<td>373</td>
</tr>
<tr>
<td>Extract all streams from OLE structured storage documents for scanning</td>
<td>375</td>
</tr>
<tr>
<td>Specify a replacement file name</td>
<td>376</td>
</tr>
<tr>
<td>Specify archive file types to scan</td>
<td>376</td>
</tr>
<tr>
<td>Modify the ICAP options attribute-list extension</td>
<td>377</td>
</tr>
<tr>
<td>Modify the ICAP response to send the nonviral threat category name</td>
<td>377</td>
</tr>
<tr>
<td>Access scan error files</td>
<td>378</td>
</tr>
<tr>
<td>Delete or repair infected read-only files</td>
<td>378</td>
</tr>
<tr>
<td>Disable automatic self-test scanning</td>
<td>379</td>
</tr>
<tr>
<td>Enable nonviral threat categories information</td>
<td>380</td>
</tr>
<tr>
<td>Specify decomposer file size limit</td>
<td>381</td>
</tr>
<tr>
<td>Specify maximum file size for extracted files</td>
<td>381</td>
</tr>
<tr>
<td>Specify maximum cumulative file size for extracted files</td>
<td>382</td>
</tr>
<tr>
<td>Specify the maximum socket timeout value</td>
<td>382</td>
</tr>
<tr>
<td>Change authentication mode settings for accessing Symantec Protection</td>
<td>383</td>
</tr>
<tr>
<td>Engine console</td>
<td></td>
</tr>
<tr>
<td>Add or change authorized group name to access Symantec Protection</td>
<td>383</td>
</tr>
<tr>
<td>Engine console</td>
<td></td>
</tr>
<tr>
<td>Add RPC clients</td>
<td>384</td>
</tr>
<tr>
<td>Configure MS Office file scanning</td>
<td>384</td>
</tr>
<tr>
<td>Specify file size threshold for scanning exclusion</td>
<td>385</td>
</tr>
<tr>
<td>Specify file size threshold for in-place scanning</td>
<td>385</td>
</tr>
<tr>
<td>Include category information from ICAP response in URL filtering</td>
<td>386</td>
</tr>
<tr>
<td>Enable subcategories description</td>
<td>386</td>
</tr>
<tr>
<td>Enable threat categories information</td>
<td>387</td>
</tr>
</tbody>
</table>
Introducing Symantec™ Protection Engine for Network Attached Storage

This chapter includes the following topics:

- About Symantec™ Protection Engine for Network Attached Storage
- What's new in Symantec Protection Engine
- Components of Symantec Protection Engine
- How Symantec Protection Engine works
- What you can do with Symantec Protection Engine
- Where to get more information

About Symantec™ Protection Engine for Network Attached Storage

Symantec™ Protection Engine for Network Attached Storage is hereafter referred to as Symantec Protection Engine.

Symantec Protection Engine is a carrier class content and URL scanning engine. Symantec Protection Engine provides content scanning and URL filtering capabilities to any application on an IP network, regardless of its platform. Any application can pass files or URLs to Symantec Protection Engine for scanning.

Symantec Protection Engine accepts scan requests from the client applications that use any of the following protocols:
What's new in Symantec Protection Engine

Table 1-1 describes the new features in Symantec Protection Engine.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced machine learning</td>
<td>Symantec Protection Engine 7.9 is now incorporated with the advanced machine learning technology that can detect malware based on static attributes. This technology enables Symantec Protection Engine to detect large classes of malware, both known, and unknown. In Symantec Protection Engine, this technology works with the File Insight (Reputation) technology to provide best-in-class protection with low false positives. See “About advanced machine learning” on page 144.</td>
</tr>
<tr>
<td>Syslog support on Linux</td>
<td>You can now configure Symantec Protection Engine 7.9 to send its log messages to Linux syslog which is a standard for message logging. See “Configuring logging to the Linux Syslog” on page 213.</td>
</tr>
</tbody>
</table>
Table 1-1  New features (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rapid Release HTTP protocol support</td>
<td>You can now configure Symantec Protection Engine 7.9 to use HTTP protocol for Rapid Release definition updates. See “Configuring Rapid Release to download definitions from HTTP Server” on page 321.</td>
</tr>
<tr>
<td>Reintroduction of user interface</td>
<td>Symantec Protection Engine 7.9 has reintroduced the user interface. You can now use the user interface to administer and configure Symantec Protection Engine. You can also use the command-line interface to configure and administer Symantec Protection Engine.</td>
</tr>
</tbody>
</table>

Components of Symantec Protection Engine

Table 1-2 lists the components that are included in the Symantec_Protection_Engine.zip file.

Table 1-2  Product components

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
<th>Folder name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Symantec Protection Engine</td>
<td>The software that you install to protect your network from threats (such as viruses), security risks (such as adware and spyware), and unwanted content.</td>
<td>Symantec_Protection_Engine\Silent_Install\</td>
</tr>
<tr>
<td>Silent installation</td>
<td>The files that you can use to perform a silent installation. Also includes response files for Red Hat.</td>
<td>Symantec_Protection_Engine\Silent_Install\</td>
</tr>
<tr>
<td>Command-line scanner</td>
<td>The software that acts as a client to Symantec Protection Engine through the Symantec Protection Engine application programming interface (API). The command-line scanner lets you send files to Symantec Protection Engine to be scanned.</td>
<td>Command_Line_Scanner\</td>
</tr>
</tbody>
</table>
Table 1-2  Product components (continued)

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
<th>Folder name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Symantec Protection Engine software developer’s kit</td>
<td>The tools and documentation that you can use to create the customized integrations that use ICAP.</td>
<td>Symantec_Protection_Engine_SDK\</td>
</tr>
</tbody>
</table>

Table 1-3 lists the components that are included in the Symantec_Protection_Engine_Tools.zip file.

Table 1-3  Product components

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
<th>Folder name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Symantec Central Quarantine server</td>
<td>The tool that you use to quarantine infected files that cannot be repaired when you use the ICAP protocol or RPC protocol. Symantec Central Quarantine server lets you isolate unrepairable files so that threats cannot spread.</td>
<td>Tools\Central_Quarantine\</td>
</tr>
<tr>
<td>LiveUpdate™ Administration Utility</td>
<td>The utility that you use to configure one or more intranet HTTP, or LAN servers to act as internal LiveUpdate servers. LiveUpdate lets Symantec products download program and definition file updates either directly from Symantec or from a LiveUpdate server.</td>
<td>Tools\LiveUpdate_Admin\</td>
</tr>
</tbody>
</table>
### Table 1-3  
Product components *(continued)*

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
<th>Folder name</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Center Operations Manager 2007 and 2012 (SCOM) Pack</td>
<td>You can integrate Symantec Protection Engine events with System Center Operations Manager (SCOM). System Center Operations Manager is a central repository that can receive critical events, errors, warnings, and other information from your Symantec Protection Engine servers. Preconfigured rules are automatically created when you import the management pack. System Center Operation Manager Agent monitors Windows Event log for Symantec Protection Engine events based on criteria mentioned in rules of Management pack. When a rule is triggered, the Operations Manager 2007 and 2012 Agent collects data about the event and forwards it to the System Center Operations Manager.</td>
<td>Tools\SCOM\Management_Pack</td>
</tr>
<tr>
<td>MIB file</td>
<td>The Management Information Base (MIB) file <em>(symantecprotectionengine.mib)</em> is located in the MIB directory in the Symantec Protection Engine Tools zip file. You can use this file to configure SNMP alerts.</td>
<td>Tools\MIB\symantecprotection\engine.mib</td>
</tr>
<tr>
<td>LiveUpdate Log Config files</td>
<td>The LiveUpdate Log Config folder contains the various configuration files to enable LiveUpdate logging on all platforms.</td>
<td>Tools\LiveUpdate\Log_Config\</td>
</tr>
</tbody>
</table>

Adobe Acrobat Reader is required to view the reports that are generated in .pdf format. You can download Adobe Acrobat Reader from [http://www.adobe.com/](http://www.adobe.com/).
How Symantec Protection Engine works

You can use one of the SDKs or build your custom application that supports ICAP to connect to Symantec Protection Engine.

You can create a custom integration using any of the following ways:

- Client-side application programming interface (API) C library
  If you plan to integrate content scanning, you can use the Symantec Protection Engine API.

- Client-side application programming interface (API) Java library
  If you plan to integrate content scanning, you can use the Symantec Protection Engine API.

- Client-side application programming interface (API) .Net library
  If you plan to integrate content scanning, you can use the Symantec Protection Engine API.

- Standard ICAP, based on the specification that is presented in RFC 3507 (April 2003)

For more information, see the Symantec Protection Engine Software Developer's Guide.

You can configure client applications to pass files to Symantec Protection Engine through one of the supported communication protocols. You can configure Symantec Protection Engine to scan only the files that it receives from the client application. The client application must decide which files to scan and what to do with the results.

You might need to configure the third party application to add threat, security risk, and URL filtering. Consult any documentation that is included with the connector in addition to this guide.

About automatic load balancing

The Symantec Protection Engine APIs provide load balancing across multiple computers that run Symantec Protection Engine. Client applications that pass files to Symantec Protection Engine benefit from load-balanced scanning without any additional effort. If you use multiple protection engines, the API determines which protection engine receives the next file to be scanned based on a scheduling algorithm.

If any Symantec Protection Engine cannot be reached or fails during a scan, another Symantec Protection Engine is called. The faulty Symantec Protection Engine is taken out of rotation for a period of time. If all of the Symantec Protection Engines are out of rotation, the faulty Symantec Protection Engines are called again.
When the number of queued requests for a Symantec Protection Engine exceeds its threshold, Symantec Protection Engine rejects the scan request. It notifies the client that the server has reached the queued request threshold. The client can then adjust the load balancing, which prevents the server from being overloaded with scan requests. This feature lets the client applications that pass files to Symantec Protection Engine benefit from load-balanced scanning without any additional effort.

See “Allocating resources for Symantec Protection Engine” on page 81.

See “Disable the ICAP threshold client notification” on page 372.

The API tries to contact Symantec Protection Engine five times within the pool of available Symantec Protection Engines.

About supported protocols for Symantec Protection Engine

Table 1-4 lists the supported protocols that client applications can use to send scan requests to Symantec Protection Engine.

Table 1-4 Supported protocols

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Content Adaptation Protocol (ICAP)</td>
<td>ICAP is a lightweight protocol for executing a remote procedure call on HTTP messages. ICAP is part of an architecture that lets corporations, carriers, and ISPs dynamically scan, change, and augment Web content as it flows through ICAP servers. The protocol lets ICAP clients pass HTTP messages to ICAP servers for adaptation. Adaptation might include some sort of transformation or other processing, such as scanning or content filtering. The server executes its transformation service on the messages and responds to the client, usually with modified messages. The adapted messages might be either HTTP requests or HTTP responses. In a typical integration, a caching proxy server retrieves the requested information from the Web. It caches the information and serves multiple requests for the same Web content from the cache, where possible. A caching proxy server can use ICAP to communicate with Symantec Protection Engine. It can also request the scanning of the content that is retrieved from the Web.</td>
</tr>
</tbody>
</table>

See “About working with ICAP” on page 97.
Table 1-4  Supported protocols (continued)

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A proprietary Remote Procedure Call (RPC) protocol</td>
<td>Remote procedure call (RPC) is a client/server infrastructure that increases the interoperability and portability of an application. RPC lets the application be distributed over multiple platforms. The use of RPC frees the developer from having to be familiar with various operating systems and network interfaces. RPC simplifies the development of applications that span multiple operating systems and network protocols. The semantics of the remote procedure call remain the same whether or not the client and server are on the same computer. Symantec Protection Engine uses a proprietary scanning protocol with the MS-RPC protocol to interface with client applications. This protocol is supported only on Windows 2008 Server, Windows 2012 Server, and Windows 2016 Server. Any appropriate client can use RPC to communicate with Symantec Protection Engine to request the scanning and repairing of files. See “About working with the RPC protocol” on page 100.</td>
</tr>
</tbody>
</table>

See “Supported services by protocol” on page 95.

What you can do with Symantec Protection Engine

Table 1-5 lists the tasks that you can perform with Symantec Protection Engine.

Table 1-5  What you can do with Symantec Protection Engine

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
</table>
| Configure protocols to pass files to Symantec Protection Engine for scanning | You can change the communication protocol that Symantec Protection Engine uses to communicate with the client applications for which it provides scanning services. The features that are available through Symantec Protection Engine differ depending on the protocol that you use. You can use any of the following protocols:
  - ICAP
  - RPC
After you select a protocol, you must provide the configuration information specific to the protocol. The configuration options differ depending on the protocol that you select. See “About the communication protocols” on page 94. |
### Table 1-5

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detect threats</td>
<td>You can configure Symantec Protection Engine to scan files and email messages for threats, such as viruses and Trojan horses. You can configure the policies to process the documents that contain threats. You can also quarantine the infected files that cannot be repaired.</td>
</tr>
<tr>
<td></td>
<td>See “Enabling threat detection in Symantec Protection Engine” on page 114.</td>
</tr>
<tr>
<td></td>
<td>See “About quarantining files in Symantec Protection Engine” on page 119.</td>
</tr>
<tr>
<td>Prevent potential</td>
<td>You can filter files and email messages to further protect your network.</td>
</tr>
<tr>
<td>threats</td>
<td>See “Configuring file size filtering in Symantec Protection Engine” on page 124.</td>
</tr>
<tr>
<td></td>
<td>See “Configuring file name filtering in Symantec Protection Engine” on page 122.</td>
</tr>
<tr>
<td></td>
<td>See “Configuring subject line content filtering in Symantec Protection Engine” on page 126.</td>
</tr>
<tr>
<td></td>
<td>See “Configuring message origin filtering in Symantec Protection Engine” on page 128.</td>
</tr>
<tr>
<td></td>
<td>Symantec Protection Engine can also block certain types of the container files that might contain threats or malicious code.</td>
</tr>
<tr>
<td></td>
<td>See “About container files in Symantec Protection Engine” on page 130.</td>
</tr>
<tr>
<td>Detect security risks</td>
<td>Symantec Protection Engine can detect security risks such as: adware, dialers, hacking tools, joke programs, remote access programs, spyware, and trackware. You can also quarantine the infected files that cannot be repaired.</td>
</tr>
<tr>
<td></td>
<td>See “Enabling nonviral threat detection in Symantec Protection Engine” on page 117.</td>
</tr>
<tr>
<td></td>
<td>See “About quarantining files in Symantec Protection Engine” on page 119.</td>
</tr>
</tbody>
</table>
### Table 1-5

**What you can do with Symantec Protection Engine**

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prevent denial-of-service</td>
<td>Symantec Protection Engine protects your network from the file attachments that can overload the system and cause denial-of-service attacks.</td>
</tr>
<tr>
<td>attachments</td>
<td>Denial-of-service attacks can include any of the following types of container files:</td>
</tr>
<tr>
<td></td>
<td>■ Files that are overly large</td>
</tr>
<tr>
<td></td>
<td>■ Files that contain large numbers of embedded, compressed files</td>
</tr>
<tr>
<td></td>
<td>■ Files that are designed to maliciously use resources and degrade performance.</td>
</tr>
<tr>
<td></td>
<td>To reduce your exposure to denial-of-service threats, you can impose limits to control how Symantec Protection Engine handles container files.</td>
</tr>
<tr>
<td></td>
<td>See “Setting container file limits” on page 161.</td>
</tr>
<tr>
<td>Specify the files to scan</td>
<td>You can conserve bandwidth and time if you limit the files and messages that are scanned.</td>
</tr>
<tr>
<td></td>
<td>See “Specifying which files to scan” on page 157.</td>
</tr>
<tr>
<td></td>
<td>See “Specifying the maximum file or message size to scan” on page 160.</td>
</tr>
<tr>
<td>Filter HTTP requests for</td>
<td>If your client uses ICAP, you can apply Uniform Resource Locator (URL) filtering to block access to sites that contain unwanted content.</td>
</tr>
<tr>
<td>unwanted content</td>
<td>Symantec Protection Engine uses Symantec URL categories and Child Abuse Image Content (CAIC) URL categories to scan and block the unwanted</td>
</tr>
<tr>
<td></td>
<td>URLs.</td>
</tr>
<tr>
<td></td>
<td>See “About categories” on page 168.</td>
</tr>
<tr>
<td>Customize user notifications</td>
<td>Symantec Protection Engine lets you customize messages to users to notify them when a file has been infected, repaired, or deleted.</td>
</tr>
<tr>
<td></td>
<td>You can add the text to the body of an infected MIME-encoded message or to the body of a replacement file for a deleted attachment.</td>
</tr>
<tr>
<td></td>
<td>See “Customizing notifications in Symantec Protection Engine” on page 135.</td>
</tr>
<tr>
<td></td>
<td>See “Customizing the access denied message” on page 190.</td>
</tr>
</tbody>
</table>
### Table 1-5 What you can do with Symantec Protection Engine (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log events and review event data and statistics</td>
<td>Symantec Protection Engine can send events to several logging destinations. You can activate logging to each available destination when you select the logging level that you want for that destination. You can then choose the logging levels for which Symantec Protection Engine generates log messages. Use the Symantec Protection Engine reporting functionality to view your log data and statistics. See “About logging data” on page 200.</td>
</tr>
<tr>
<td>Issue alerts</td>
<td>Symantec Protection Engine can send alerts through Simple Mail Transfer Protocol (SMTP) and Simple Network Management Protocol (SNMP). You also can activate outbreak alerts. Symantec Protection Engine can issue alerts when a certain number of the same types of threat or violations occur in a given time interval. Outbreak alerts provide an early warning of a potential outbreak so that you can take the necessary precautions to protect your network. See “About configuring alerts” on page 213.</td>
</tr>
<tr>
<td>Monitor Symantec Protection Engine performance</td>
<td>You can monitor Symantec Protection Engine to ensure that it operates at an optimal level for your environment. Continual monitoring ensures that you can make the necessary adjustments as soon as you detect a degradation in performance. See “How to monitor Symantec Protection Engine performance” on page 145.</td>
</tr>
<tr>
<td>Keep your protection up-to-date</td>
<td>You can update your content for Symantec Protection Engine. Content updates ensure that your network is up-to-date with the most current risk and URL definitions. You also can update Symantec Protection Engine with the latest definitions without any interruption to scanning or filtering operations. See “About content updates” on page 226.</td>
</tr>
</tbody>
</table>
Table 1-5  What you can do with Symantec Protection Engine (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Perform tasks from the command-line scanner</td>
<td>The command-line scanner acts as a client to Symantec Protection Engine through the Symantec Protection Engine API. Use the command-line scanner to send files to Symantec Protection Engine to be scanned for threats. The command-line scanner also lets you take the following actions: ■ Repair infected files and delete those files that are unrepairable ■ Recursively descend into the subdirectories to scan multiple files ■ Provide output information about the command-line scanner and protection engine operation. See “About the Symantec Protection Engine command-line scanner” on page 337.</td>
</tr>
</tbody>
</table>

Where to get more information

Symantec Protection Engine includes an online Help system. You can access topics through the Help table of contents and index, and you can search for keywords. Context-sensitive help is available for each page in the Symantec Protection Engine console.

You can visit the Symantec Web site for more information about our product.

The following online resources are available:

- Provides access to the technical support Knowledge Base, newsgroups, contact information, downloads, and mailing list subscriptions  
  https://support.symantec.com/en_US.html
- Provides information about registration, frequently asked questions, how to respond to error messages, and how to contact Symantec License Administration  
  http://customersupport.symantec.com/
- Provides product news and updates  
  https://www.symantec.com/
- Provides access to the Virus Encyclopedia, which contains information about all known threats, information about hoaxes, and access to white papers about threats  
  https://www.symantec.com/security_response/
Installing Symantec Protection Engine

This chapter includes the following topics:

■ Before you install Symantec Protection Engine
■ System requirements
■ About installing Symantec Protection Engine
■ Symantec Protection Engine post-installation tasks
■ Migrating to version 7.9
■ Uninstalling Symantec Protection Engine

Before you install Symantec Protection Engine

Install Symantec Protection Engine on a computer that meets the system requirements. Before you install Symantec Protection Engine, install and configure the operating system software and applicable updates for your server. Also ensure that your operating system software and server work correctly. For more information, see the documentation for your server.

See “System requirements” on page 30.

Before you install Symantec Protection Engine, take the following steps:

■ On Windows operating system, if you want to use Windows Active Directory-based authentication method to access the Symantec Protection Engine console, you must ensure the following:
  ■ Create or identify an existing security group in the Active Directory that would be authorized to access the Symantec Protection Engine console.
The server (on which you plan to install Symantec Protection Engine) belongs to the same domain or has trust relationship with the Active Directory, that contains the security group authorized to access the Symantec Protection Engine console.

Install Java 2SE Runtime Environment (JRE) 8.0 (update 121 or later) 64-bit on Windows and Linux platform server.

Disable any third party antivirus products that are running on the server on which you plan to install Symantec Protection Engine. You can turn on antivirus protection after installation is complete. Symantec Protection Engine scans the files that client applications pass to Symantec Protection Engine. Symantec Protection Engine does not protect the computer on which it runs. Since Symantec Protection Engine processes the files that might contain threats, the server on which it runs is vulnerable if it has no real-time protection.

Use an antivirus program to protect the server on which Symantec Protection Engine runs, such as Symantec Endpoint Protection. To prevent scanning conflicts, configure the antivirus program not to scan the temporary directory that Symantec Protection Engine uses for scanning.

Review the deployment considerations and recommendations. These recommendations can enhance your overall performance. See “Deployment considerations and recommendations” on page 154.

After you complete the installation, perform the post-installation tasks. See “Symantec Protection Engine post-installation tasks” on page 61.

System requirements

Before you install Symantec Protection Engine, verify that your server meets the minimum system requirements.

- System requirements to install Symantec Protection Engine on Windows
- System requirements to install Symantec Protection Engine on Linux

For Symantec Protection Engine platform support matrix, see the following pages:

- Symantec Protection Engine for Cloud Services
- Symantec Protection Engine for Network Attached Storage
System requirements to install Symantec Protection Engine on Windows

The minimum system requirements to install Symantec Protection Engine on Windows are as follows:

**Operating system**
- Windows Server 2008 SP2 (64-bit)
- Windows Server 2008 R2 (64-bit)
- Windows Server 2012 (64-bit)
- Windows Server 2012 R2 (64-bit)
- Windows Server 2008 SP2 (64-bit) Japanese
- Windows Server 2008 R2 (64-bit) Japanese
- Windows Server 2012 (64-bit) Japanese
- Windows Server 2012 R2 (64-bit) Japanese
- Windows Server 2016 (64-bit)

Ensure that your operating system has the latest service patches available.

**Processor**
Intel or AMD Server Grade Single Processor Quad Core systems or higher

**Memory**
8 GB RAM or higher

**Disk space**
40 GB of hard disk space
60 GB of hard disk space for using URL Filtering feature

**Hardware**
- Network interface card (NIC) running TCP/IP with a static IP address
- Internet connection to update definitions
- 100 Mbps Ethernet link (1 Gbps recommended)
Software

- Java 2SE Runtime Environment (JRE) 8.0 (update 121 or later)
  64-bit
  You must install JRE only if you plan to operate Symantec Protection
  Engine in the Core server with user interface mode.
- Microsoft Visual C++ 2010 Redistributable Package (x64)
- One of the following Web browsers to access the Symantec
  Protection Engine console:
  - Microsoft Internet Explorer 11 or later
    Use Microsoft Internet Explorer to access the Symantec
    Protection Engine console from a Windows client computer.
    **Note:** If you are using 64-bit Internet Explorer browser, you must
    add the following registry key:
    `\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet
    Explorer\MAIN\"TabProcGrowth"=dword:00000000`
  - Mozilla Firefox 32-bit (Extended Support Release) 45 or later
    Use Mozilla Firefox to access the Symantec Protection Engine
    console from a Linux client computer.

The Web browser is required only for Web-based administration.
You must install the Web browser on a computer from which you
want to access the Symantec Protection Engine console. The
computer must have access to the server on which Symantec
Protection Engine runs.

Hypervisor support

- Windows 2008 R2 Hyper-V
- Windows 2012 Hyper-V
- VMware vsphere 5.5 or later
- VMware vsphere 6.0 or later

The following Windows guest operating systems have been certified
on Hyper-V:

- Windows Server 2008 SP2 (64-bit)
- Windows Server 2008 R2 (64-bit)
- Windows Server 2008 Japanese (64-bit)
- Windows Server 2008 R2 Japanese (64-bit)
- Windows Server 2012 (64-bit)
- Windows Server 2016 (64-bit)

System requirements to install Symantec Protection Engine on Linux

The minimum system requirements to install Symantec Protection Engine on Linux
are as follows:
| **Operating system** | Red Hat Enterprise Linux Server 5.10 (64-bit) or later  
| | Red Hat Enterprise Linux Advanced Server 5.10 (64-bit) or later  
| | Red Hat Enterprise Linux Server 6.7 (64-bit) or later  
| | Red Hat Enterprise Linux Server 6.8 (64-bit) or later  
| | Red Hat Enterprise Linux Server 7.0 (64-bit) or later  
| | Red Hat Enterprise Linux Server 7.1 (64-bit) or later  
| | Red Hat Enterprise Linux Server 7.2 (64-bit) or later  
| | SUSE Linux Enterprise Server 11 (64-bit)  
| | SUSE Linux Enterprise Server 12 (64-bit)  
| | CentOS Linux 7.1 (64-bit) or later  
| | CentOS Linux 7.2 (64-bit) or later  

Ensure that your operating system has the latest service patches available.

| **Processor** | Intel or AMD Server Grade Single Processor Quad Core systems or higher |
| **Memory** | 8 GB RAM or higher |
| **Disk space** | 40 GB of hard disk space  
| | 60 GB of hard disk space for using URL Filtering feature |

| **Hardware** | Network interface card (NIC) running TCP/IP with a static IP address  
| | Internet connection to update definitions  
| | 100 Mbps Ethernet link (1 Gbps recommended) |
Software

- Ensure that the following packages are installed:
  - 64-bit zlib library package
  - GNU sharutils-4.6.1-2 or later
    Use this package to expand the Rapid Release packages.
  - 64-bit GNU libuuid-2.17.2-6 or later
  - ncompress-4.2.4-44 or later
    Use this package to expand the Rapid Release packages.
  - FTP package
    Use this package to download Rapid Release definitions.
  - 64-bit GNU C Library (glibc)
  - Initscripts
    This package is required for Red Hat Linux only.
  - aaa_base package
    This package is required for SUSE only.
  - Java 2SE Runtime Environment (JRE) 8.0 (update 121 or later)
    64-bit
    You must install JRE only if you plan to operate Symantec Protection Engine in the Core server with user interface mode.
    Install JRE using Red Hat Package Manager (RPM). Ensure that you note the installation location. You must provide the location of the JRE if the installer is unable to detect it.
  - One of the following Web browsers to access the Symantec Protection Engine console:
    - Microsoft Internet Explorer 11 or later
      Use Microsoft Internet Explorer to access the Symantec Protection Engine console from a Windows client computer.
      **Note:** If you are using 64-bit Internet Explorer browser, you must add the following registry key:
      
      [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\MAIN] "TabProcGrowth"=dword:00000000
    - Mozilla Firefox 32-bit (Extended Support Release) 45 or later
      Use Mozilla Firefox to access the Symantec Protection Engine console from a Linux client computer.
      The Web browser is required only for Web-based administration. You must install the Web browser on a computer from which you want to access the Symantec Protection Engine console. The computer must have access to the server on which Symantec Protection Engine runs.
      **Note:** If any of the above package binary is already present on the computer and if the installer is still unable to find it, you can add the path to the binary in LD_LIBRARY_PATH environment variable.
Hypervisor support
- Windows 2008 R2 Hyper-V
- Windows 2012 Hyper-V
- VMware vsphere 5.5 or later
- VMware vsphere 6.0 or later

The following Linux guest operating systems have been certified on Hyper-V:
- Red Hat Enterprise Linux Server 5.10 (64-bit)
- Red Hat Enterprise Linux Server 6.2 or later (64-bit)
- Red Hat Enterprise Linux Server 6.7 (64-bit)
- SUSE Linux Enterprise Server 11 (64-bit)
- Centos 7.1 or later

About installing Symantec Protection Engine

The Symantec Protection Engine installer checks for the previous version of the product before installing or upgrading to a newer version. The results of the check determine what happens next.

Table 2-1 describes the action taken by the installer when no previous version is installed or an existing version of Symantec Protection Engine is installed.

<table>
<thead>
<tr>
<th>Version</th>
<th>Action taken by installer</th>
</tr>
</thead>
<tbody>
<tr>
<td>No previous version is</td>
<td>A full installation is performed.</td>
</tr>
<tr>
<td>detected</td>
<td></td>
</tr>
<tr>
<td>Version 7.8.x is detected</td>
<td>Symantec Protection Engine 7.9 supports an upgrade from version 7.8.x. You can choose to upgrade the product and preserve your existing settings or perform a clean upgrade. If you choose to do a clean upgrade, the installer removes the previous version, and then installs the newer version as a full installation, without preserving any previous settings.</td>
</tr>
<tr>
<td>Version 7.5 is detected</td>
<td>Symantec Protection Engine does not support direct upgrades from version 7.5.x. You must first migrate to version 7.8.0. A separate utility to migrate from 7.5.x to 7.8.0 is provided. For more information, see the Symantec Protection Engine 7.8.0 Migration Utility at the following location: <a href="https://support.symantec.com/en_US/article.INFO3603.html">https://support.symantec.com/en_US/article.INFO3603.html</a></td>
</tr>
</tbody>
</table>

Table 2-1: Installer check results
After you install Symantec Protection Engine, activate all applicable licenses. If you upgrade from a previous version that has valid licenses, when the installation is complete, Symantec Protection Engine automatically recognizes these licenses.

See “About licensing” on page 88.

Symantec Protection Engine is shipped with the minimum set of URL definitions. If you want to use URL filtering feature, ensure that you run LiveUpdate and get the latest URL definitions before you start URL filtering.

See “About filtering URLs” on page 167.

If Symantec Protection Engine fails to start before it can initiate standard logging, information about the failure is written to the abort log file (SymantecProtectionEngineAbortLog.txt). This file is located in the installation directory.

If you need to install or upgrade multiple Symantec Protection Engines on your network, you can use the silent installation or upgrade feature to facilitate the process.

See “About silent installation and upgrade” on page 325.

See “About authentication modes in Symantec Protection Engine” on page 36.

See "Installing Symantec Protection Engine on Windows " on page 37.

See "Installing Symantec Protection Engine on Linux" on page 53.

### About authentication modes in Symantec Protection Engine

During installation of Symantec Protection Engine, you can choose the authentication mode for accessing the Symantec Protection Engine console.

You can choose any one of the following authentication modes to access Symantec Protection Engine console:

---

**Table 2-1** Installer check results *(continued)*

<table>
<thead>
<tr>
<th>Version</th>
<th>Action taken by installer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 7.0 is detected</td>
<td>Symantec Protection Engine does not support direct upgrades from version 7.0.x. You must first upgrade to version 7.5.x.</td>
</tr>
<tr>
<td>Version 5.1 or 5.2 is detected</td>
<td>Symantec Protection Engine does not support direct upgrades from version 5.1 or 5.2. You must first upgrade to version 7.0.x.</td>
</tr>
<tr>
<td>Version 5.0 is detected</td>
<td>Symantec Protection Engine does not support direct upgrades from version 5.0. You must first upgrade to version 7.0.x.</td>
</tr>
</tbody>
</table>
Users can access the Symantec Protection Engine console using Symantec Protection Engine user password. This authentication mode is available for Windows and non-Windows platforms.

Users from the authorized domain and security group can access the Symantec Protection Engine console using their Windows Active Directory credentials. This authentication mode is available only for Windows platforms.

See “About installing Symantec Protection Engine” on page 35.
See “Installing Symantec Protection Engine on Windows” on page 37.
See “Installing Symantec Protection Engine on Linux” on page 53.

Installing Symantec Protection Engine on Windows

During installation, you can choose the authentication mode for accessing the Symantec Protection Engine console. If you choose Symantec Protection Engine-based authentication then Symantec Protection Engine installs with an administrator account. Symantec recommends that you remember the password for this account as it is the only account used to manage Symantec Protection Engine. If you want to change the password in the console, you must have the old password.

If you choose Windows Active Directory-based authentication, Symantec Protection Engine allows users from the authorized Windows Active Directory security group to access the console.

See “About authentication modes in Symantec Protection Engine” on page 36.
See “Accessing the Symantec Protection Engine console” on page 65.

Before you begin the installation process, ensure that your computer meets the minimum system requirements.

See “System requirements” on page 30.

Note: Symantec recommends that you install Symantec Protection Engine with Administrative or equivalent privilege account. Also, for security purposes, the read, write, and execute permissions for all Symantec Protection Engine-based files should be denied for all other users.
When the installation is complete, Symantec Protection Engine is installed as a Windows 2008, 2012, or 2016 service. It is listed as Symantec Protection Engine in the Services Console. The Symantec Protection Engine service starts automatically when the installation is complete. Any significant installation activities are recorded in the Windows Application Event Log.

Select one of the following procedures for the type of installation or upgrade that you want to perform:

- **First time product installation**
  See “To install Symantec Protection Engine on Windows with Symantec Protection Engine-based authentication” on page 38.
  See “To install Symantec Protection Engine on Windows with Windows Active Directory-based authentication” on page 41.

- **Upgrade from a previous version and retain existing settings**

- **Perform a clean upgrade**
  Uninstalls your current version of Symantec Protection Engine and installs the newer version. However, any settings that you made to Symantec Protection Engine are lost during the upgrade.
  See “To configure Symantec Protection Engine clean upgrade installation option on Windows with Symantec Protection Engine-based authentication” on page 44.
  See “To configure Symantec Protection Engine clean upgrade installation options on Windows with Active Directory-based authentication” on page 46.

- **Perform a preserved settings upgrade**
  Uninstalls your current version of Symantec Protection Engine and installs the newer version, while preserving your existing settings.
  See “Configuring the preserve settings upgrade installation option on Windows” on page 49.

**To install Symantec Protection Engine on Windows with Symantec Protection Engine-based authentication**

1. Log on to the computer on which you plan to install Symantec Protection Engine as administrator or as a user with administrator rights.
2. In the Symantec Protection Engine.zip file, run SymantecProtectionEngine.exe.
3. In the Welcome panel, click Next.
4 In the **License Agreement** panel, after you read the agreement, indicate that you agree with the terms of the Symantec Software License Agreement, and then click **Next**.

The default setting is that you do not agree with the terms of the Symantec Software License Agreement. If you do not indicate that you agree, the installation is canceled.

5 In the **Destination Folder** panel, select the location to install Symantec Protection Engine, and then click **Next**.

The default location is C:\Program Files\Symantec\Scan Engine.

---

**Note:** If you plan to change the default location to install Symantec Protection Engine, make sure the new directory has the same permissions as that of the Program Files directory.

---

**Warning:** If the new location to install Symantec Protection Engine does not have the same permissions as that of the Program Files directory, malicious users with lower privilege can read and copy file contents, replace malicious data in tags, rename the file, or even delete the product files.

6 In the **Initialization Methods** panel, select one of the following options, and click **Next**:

- **Core server with user interface (requires JRE)**
  
  Select this option if you want to use the user-interface console of Symantec Protection Engine.

  This method requires JRE to be installed.

  Proceed to step 7.

- **Core server only (does not require JRE)**
  
  Select this option if you do not want to use the user-interface console of Symantec Protection Engine.

  This method does not require JRE to be installed.

  Proceed to step 12.

7 In the **UI Authentication method** panel, select **Symantec Protection Engine-based authentication**, and then click **Next**.
8 In the **Administrative UI Setup** panel, configure the following options:

- **Administrator Password**
  - Type a password for the administrator account that you intend to use to manage Symantec Protection Engine.
  - Confirm Administrator Password
  - Confirm the password by typing it again.

9 Click **Next**.

10 In the **Administrative UI Setup** panel, configure the following options:

- **Administrator Port**
  - Type the port number on which the Web-based console listens.
  - If you change the port number, use a number that is greater than 1024 that is not in use by any other program or service. The default port number is 8004. You can disable the console by typing 0. If you disable the console, you can configure Symantec Protection Engine by editing the configuration file.
  - See "About editing the Symantec Protection Engine configuration files" on page 365.

- **SSL Port**
  - Type the Secure Socket Layer (SSL) port number on which encrypted files are transmitted for increased security.
  - The default SSL port number is 8005. If this port is already in use, select an SSL port that is not in use by any other program or service. Use a port number that is greater than 1024.

11 Click **Next**.

12 In the **URL Filtering and URL Reputation** panel, select **Enable URL Filtering and download URL Filtering definitions** to enable URL filtering feature.

- Select **Enable URL Reputation and download URL Reputation definitions** to enable URL Reputation feature.

13 Click **Next**.

14 In the **Reputation-based Protection (Insight)** panel, select the **Insight Aggression Level** from the list.

- The Insight aggression level defines how sensitive the Symantec Insight™ feature is to a file’s reputation score.
  - See “Configuring the Symantec Insight™ aggression level” on page 142.

15 In the **Ready to Install the Program** panel, click **Install**.

16 Click **Finish**.
To install Symantec Protection Engine on Windows with Windows Active Directory-based authentication

1. Log on to the computer on which you plan to install Symantec Protection Engine as administrator or as a user with administrator rights.

2. In the Symantec Protection Engine.zip file, run SymantecProtectionEngine.exe.

3. In the Welcome panel, click Next.

4. In the License Agreement panel, after you read the agreement, indicate that you agree with the terms of the Symantec Software License Agreement, and then click Next.

   The default setting is that you do not agree with the terms of the Symantec Software License Agreement. If you do not indicate that you agree, the installation is canceled.

5. In the Destination Folder panel, select the location to install Symantec Protection Engine, and then click Next.

   The default location is C:\Program Files\Symantec\Scan Engine.

   **Note:** If you plan to change the default location to install Symantec Protection Engine, make sure the new directory has the same permissions as that of the Program Files directory.

   **Warning:** If the new location to install Symantec Protection Engine does not have the same permissions as that of the Program Files directory, malicious users with lower privilege can read and copy file contents, replace malicious data in tags, rename the file, or even delete the product files.
6 In the **Initialization Methods** panel, select one of the following options, and click **Next**:

- **Core server with user interface (requires JRE)**
  - Select this option if you want to use the user-interface console of Symantec Protection Engine.
  - This method requires you to install JRE.
  - Proceed to step 7.

- **Core server only (does not require JRE)**
  - Select this option if you do not want to use the user-interface console of Symantec Protection Engine.
  - This method does not require JRE to be installed.
  - Proceed to step 12.

7 In the **UI Authentication method** panel, select **Windows Active Directory-based authentication**, and then click **Next**.

8 In the **Windows Active Directory-based Authentication Settings** panel, in the **Group Name** box, type a valid security group name in the **Domain\Groupname** format.

9 Click **Next**.

   If the group name is incorrect, a **Group Name Validation** screen appears.

   Click **Back** to try the security group name again.

   Alternatively, click **Next** to continue the installation without a valid group name.

   The Symantec Protection Engine service starts after installation but you cannot access the console. Once the installation is complete, you must go to configuration.xml and enter a valid security group name in the **Domain\Groupname** format to access the console.
10 In the **Administrative UI Setup** panel, configure the following options:

**Administrator Port**  
Type the port number on which the Web-based console listens.  
If you change the port number, use a number that is greater than 1024 that is not in use by any other program or service. The default port number is 8004. You can disable the console by typing 0. If you disable the console, you can configure Symantec Protection Engine by editing the configuration file.

**SSL Port**  
Type the Secure Socket Layer (SSL) port number on which encrypted files are transmitted for increased security.  
The default SSL port number is 8005. If this port is already in use, select an SSL port that is not in use by any other program or service. Use a port number that is greater than 1024.

11 Click **Next**.

12 In the **URL Filtering and URL Reputation** panel, select **Enable URL Filtering** and download URL Filtering definitions to enable URL filtering feature.

Select **Enable URL Reputation and download URL Reputation definitions** to enable URL Reputation feature.

13 Click **Next**.

14 In the **Reputation-based Protection (Insight)** panel, select the **Insight Aggression Level** from the list.

The Insight aggression level defines how sensitive the Symantec Insight™ feature is to a file's reputation score.

See “Configuring the Symantec Insight™ aggression level” on page 142.

15 In the **Ready to Install the Program** panel, click **Install**.

16 Click **Finish**.

See “About the Core server only mode” on page 249.

See “Add or change authorized group name to access Symantec Protection Engine console” on page 383.

See “About installing Symantec Protection Engine” on page 35.

### Upgrading Symantec Protection Engine on Windows

You can upgrade Symantec Protection Engine from the existing version on your computer to a newer version. You can either preserve existing settings or perform a clean upgrade. If you cancel the installation process during an upgrade, you might
need to restart the service as the service stops when the installer detects an upgrade.

See “Configuring the clean upgrade installation option on Windows” on page 44. to upgrade Symantec Protection Engine using the clean upgrade installation option.

See “Configuring the preserve settings upgrade installation option on Windows” on page 49. to upgrade Symantec Protection Engine using the preserve settings upgrade installation option.

See “About installing Symantec Protection Engine” on page 35.

See “Installing Symantec Protection Engine on Windows ” on page 37.

Configuring the clean upgrade installation option on Windows

The clean upgrade option uninstalls the previous version of Symantec Protection Engine and installs the newer version. During clean upgrade installation, you can select the authentication option to access the Symantec Protection Engine console. You can select either Symantec Protection Engine-based authentication or Windows Active Directory-based authentication.

To configure Symantec Protection Engine clean upgrade installation option on Windows with Symantec Protection Engine-based authentication

1. Log on to the computer on which you plan to install Symantec Protection Engine as administrator or as a user with administrator rights.

2. In the Symantec Protection Engine .zip file, run SymantecProtectionEngine.exe.

3. In the Welcome panel, click Next.

4. In the License Agreement panel, after you read the agreement, indicate that you agree with the terms of the Symantec Software License Agreement, and then click Next.

   The default value is that you do not agree with the terms of the Symantec Software License Agreement. If you do not indicate that you agree, the installation is canceled.

5. In the Upgrade the Symantec Protection Engine panel, select Clean upgrade, and then click Next.
6 In the **Destination Folder** panel, select the location to install Symantec Protection Engine, and then click **Next**.

The default location is C:\Program Files\Symantec\Scan Engine.

---

**Note:** If you plan to change the default location to install Symantec Protection Engine, make sure the new directory has the same permissions as that of the Program Files directory.

---

**Warning:** If the new location to install Symantec Protection Engine does not have the same permissions as that of the Program Files directory, malicious users with lower privilege can read and copy file contents, replace malicious data in tags, rename the file, or even delete the product files.

7 In the **Initialization Methods** panel, select one of the following options, and click **Next**:

- **Core server with user interface (requires JRE)**
  - Select this option if you want to use the user-interface console of Symantec Protection Engine.
  - This method requires you to install JRE.
  - Proceed to step 8.

- **Core server only (does not require JRE)**
  - Select this option if you do not want to use the user-interface console of Symantec Protection Engine.
  - This method does not require JRE to be installed.
  - Proceed to step 13.

8 In the **UI Authentication method** panel, select **Symantec Protection Engine-based authentication**, and then click **Next**.

9 In the **Administrative UI Setup** panel, configure the following options:

- **Administrator Password**
  - Type a password for the administrative account that you intend to use to manage Symantec Protection Engine.

- **Confirm Administrator Password**
  - Confirm the password by typing it again.

10 Click **Next**.
11 In the **Administrative UI Setup** panel, configure the following options:

- **Administrator Port**
  Type the port number on which the Web-based console listens. If you change the port number, use a number that is greater than 1024 that is not in use by any other program or service. The default port number is 8004. You can disable the console by typing 0. If you disable the console, you can configure Symantec Protection Engine by editing the configuration file. See “About editing the Symantec Protection Engine configuration files” on page 365.

- **SSL Port**
  Type the Secure Socket Layer (SSL) port number on which encrypted files are transmitted for increased security. The default SSL port number is 8005. If this port is already in use, select an SSL port that is not in use by any other program or service. Use a port number that is greater than 1024.

12 Click Next.

13 In the **URL Filtering and URL Reputation** panel, select **Enable URL Filtering** and download URL Filtering definitions to enable URL filtering feature. Select **Enable URL Reputation and download URL Reputation definitions** to enable URL Reputation feature.

14 In the Reputation-based Protection (Insight) panel, select the **Select Insight Aggression Level** from the list. The Insight aggression level defines how sensitive the Symantec Insight™ feature is to a file's reputation score. See “Configuring the Symantec Insight™ aggression level” on page 142.

15 In the **Ready to Install the Program** panel, click Install.

16 Click Finish.

To configure Symantec Protection Engine clean upgrade installation options on Windows with Active Directory-based authentication

1 Log on to the computer on which you plan to install Symantec Protection Engine as administrator or as a user with administrator rights.

2 In the Symantec Protection Engine.zip file, run SymantecProtectionEngine.exe.

3 In the **Welcome** panel, click Next.
4 In the License Agreement panel, after you read the agreement, indicate that you agree with the terms of the Symantec Software License Agreement, and then click Next.

The default value is that you do not agree with the terms of the Symantec Software License Agreement. If you do not indicate that you agree, the installation is canceled.

5 In the Upgrade the Protection Engine panel, select Clean upgrade, and then click Next.

6 In the Destination Folder panel, select the location to install Symantec Protection Engine, and then click Next.

The default location is C:\Program Files\Symantec\Scan Engine.

Note: If you plan to change the default location to install Symantec Protection Engine, make sure the new directory has the same permissions as that of the Program Files directory.

Warning: If the new location to install Symantec Protection Engine does not have the same permissions as that of the Program Files directory, malicious users with lower privilege can read and copy file contents, replace malicious data in tags, rename the file, or even delete the product files.

7 In the Initialization Methods panel, select one of the following options, and click Next:

Core server with user interface (requires JRE) Select this option if you want to use the user-interface console of Symantec Protection Engine.

This method requires you to install JRE.

Proceed to step 8

Core server only (does not require JRE) Select this option if you do not want to use the user-interface console of Symantec Protection Engine.

This method does not require JRE to be installed.

Proceed to step 13.

8 In the UI Authentication method panel, select Windows Active Directory-based authentication, and then click Next.
9 In the **Windows Active Directory-based Authentication Settings** panel, in the **GroupName** box, type a valid security group name in the Domain\Groupname format.

10 Click **Next**.

If the group name is incorrect, an **Group Name Validation** screen appears.

Click **Back** to try the security group name again.

Alternatively, click **Next** to continue the installation without a valid security group name.

The Symantec Protection Engine service starts after installation but you cannot access the console. Once the installation is complete, you must go to configuration.xml and enter a valid security group name in the Domain\Groupname format to access the console.

11 In the **Administrative UI Setup** panel, configure the following options:

- **Administrator Port**
  - Type the port number on which the Web-based console listens.
  - If you change the port number, use a number that is greater than 1024 that is not in use by any other program or service. The default port number is 8004. You can disable the console by typing 0. If you disable the console, you can configure Symantec Protection Engine by editing the configuration file.

- **SSL Port**
  - Type the Secure Socket Layer (SSL) port number on which encrypted files are transmitted for increased security.
  - The default SSL port number is 8005. If this port is already in use, select an SSL port that is not in use by any other program or service. Use a port number that is greater than 1024.

12 Click **Next**.

13 In the **URL Filtering and URL Reputation** panel, select **Enable URL Filtering and download URL Filtering definitions** to enable URL filtering feature.

Select **Enable URL Reputation and download URL Reputation definitions** to enable URL Reputation feature.

14 In the **Reputation-based Protection (Insight)** panel, select the **Insight Aggression Level** from the list.

The Insight aggression level defines how sensitive the Symantec Insight™ feature is to a file's reputation score.

See “Configuring the Symantec Insight™ aggression level” on page 142.
In the Ready to Install the Program panel, click Install.

Click Finish.

See “Upgrading Symantec Protection Engine on Windows” on page 43.

See “About adding or changing authorized group name to access the Symantec Protection Engine console” on page 64.

See “Add or change authorized group name to access Symantec Protection Engine console” on page 383.

See “About installing Symantec Protection Engine” on page 35.

See “Installing Symantec Protection Engine on Windows” on page 37.

Configuring the preserve settings upgrade installation option on Windows

The preserved settings upgrade options uninstalls the existing version of Symantec Protection Engine and installs the newer version.

To configure Symantec Protection Engine with the preserve upgrade installation option on Windows with Symantec Protection Engine-based authentication

1 Log on to the computer on which you plan to install Symantec Protection Engine as administrator or as a user with administrator rights.

2 In the Symantec Protection Engine.zip file, run SymantecProtectionEngine.exe.

3 In the Welcome panel, click Next.

4 In the License Agreement panel, after you read the agreement, indicate that you agree with the terms of the Symantec Software License Agreement, and then click Next.

The default value is that you do not agree with the terms of the Symantec Software License Agreement. If you do not indicate that you agree, the installation is canceled.

5 In the Upgrade the Protection Engine panel, select Upgrade and preserve existing settings, configuration and data, and then click Next.
6 In the **Initialization Methods** panel, select one of the following options, and click **Next**:

- **Core server with user interface (requires JRE)**
  - Select this option if you want to use the user-interface console of Symantec Protection Engine.
  - This method requires you to install JRE.
  - Proceed to step 7.

- **Core server only (does not require JRE)**
  - Select this option if you do not want to use the user-interface console of Symantec Protection Engine.
  - This method does not require JRE to be installed.
  - Proceed to step 12.

7 In the **UI Authentication method** panel, select **Symantec Protection Engine-based authentication**, and then click **Next**.

8 In the **Administrative UI Setup** panel, configure the following options:

- **Administrator Password**
  - Type a password for the administrative account that you intend to use to manage Symantec Protection Engine.

- **Confirm Administrator Password**
  - Confirm the password by typing it again.

9 Click **Next**.
10 In the **Administrative UI Setup** panel, configure the following options:

<table>
<thead>
<tr>
<th><strong>Administrator Port</strong></th>
<th>Type the port number on which the web-based console listens.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>If you change the port number, use a number that is greater than 1024 that is not in use by any other program or service. The default port number is 8004. You can disable the console by typing 0. If you disable the console, you can configure Symantec Protection Engine by editing the configuration file.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>SSL Port</strong></th>
<th>Type the Secure Socket Layer (SSL) port number on which encrypted files are transmitted for increased security.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The default SSL port number is 8005. If this port is already in use, select an SSL port that is not in use by any other program or service. Use a port number that is greater than 1024.</td>
</tr>
</tbody>
</table>

11 Click **Next**.

12 In the **Ready to Install the Program** panel, click **Install**.

13 Click **Finish**.

To configure Symantec Protection Engine with the preserve upgrade installation option on Windows with Active Directory-based authentication

1 Log on to the computer on which you plan to install Symantec Protection Engine as administrator or as a user with administrator rights.

2 In the Symantec Protection Engine.zip file, run `SymantecProtectionEngine.exe`.

3 In the **Welcome** panel, click **Next**.

4 In the **License Agreement** panel, after you read the agreement, indicate that you agree with the terms of the Symantec Software License Agreement, and then click **Next**.

   The default value is that you do not agree with the terms of the Symantec Software License Agreement. If you do not indicate that you agree, the installation is canceled.

5 In the **Upgrade the Protection Engine** panel, select **Upgrade and preserve existing settings, configuration and data**, and then click **Next**.
6 In the **Initialization Methods** panel, select one of the following options, and click **Next**:

- **Core server with user interface (requires JRE)**
  Select this option if you want to use the user-interface console of Symantec Protection Engine.
  This method requires you to install JRE.
  Proceed to step 7.

- **Core server only (does not require JRE)**
  Select this option if you do not want to use the user-interface console of Symantec Protection Engine.
  This method does not require JRE to be installed.
  Proceed to step 13.

7 In the **UI Authentication method** panel, select **Windows Active Directory-based authentication**, and then click **Next**.

8 In the **Windows Active Directory-based Authentication Settings** panel, in the **GroupName** box, type a valid security group name in the Domain\GroupName format.

9 Click **Next**.

10 If the group name is incorrect, an **Group Name Validation** screen appears.

   Click **Back** to try the security group name again.

   Alternatively, click **Next** to continue the installation without a valid security group name.

   The Symantec Protection Engine service starts after installation but you cannot access the console. Once the installation is complete, you must go to configuration.xml and enter a valid security group name in the Domain\GroupName format to access the console.
In the **Administrative UI Setup** panel, configure the following options:

**Administrator Port**  
Type the port number on which the web-based console listens.  
If you change the port number, use a number that is greater than 1024 that is not in use by any other program or service.  
The default port number is 8004. You can disable the console by typing 0. If you disable the console, you can configure Symantec Protection Engine by editing the configuration file.

**SSL Port**  
Type the Secure Socket Layer (SSL) port number on which encrypted files are transmitted for increased security.  
The default SSL port number is 8005. If this port is already in use, select an SSL port that is not in use by any other program or service. Use a port number that is greater than 1024.

12 Click **Next**.

13 In the **Ready to Install the Program** panel, click **Install**.

14 Click **Finish**.

See “**Symantec Protection Engine post-installation tasks**” on page 61.

### Installing Symantec Protection Engine on Linux

You can install Symantec Protection Engine to run with the rights and privileges of a system user other than root or superuser.

Select one of the following procedures for the type of installation or upgrade that you want to perform:

- **First time product installation**  
  See “**To install Symantec Protection Engine on Linux**” on page 54.

- **Upgrade from a previous version and retain existing settings**  
  See “**Upgrading Symantec Protection Engine on Linux**” on page 56.

- **Perform a clean upgrade**  
  Uninstalls your current version of Symantec Protection Engine and installs the newer version.
Perform a preserved settings upgrade

Uninstalls your current version of Symantec Protection Engine and installs the newer version, while preserving your existing settings.

See “Upgrading Symantec Protection Engine on Linux” on page 56.
See “Configuring preserve settings upgrade installation options on Linux” on page 59.

To install Symantec Protection Engine on Linux

1 Log in to the computer on which you want to install Symantec Protection Engine as root.

2 Change directories to the location where the SymantecProtectionEngine.sh file is located in the product.zip file.

3 Type the following command:

```
./SymantecProtectionEngine.sh
```

4 Press y to continue with the interactive installation.

5 After you review with the Symantec License Agreement, press y to indicate that you agree with the terms of the agreement.

   If you indicate n, the installation is canceled.

6 Select the location to install Symantec Protection Engine, and then press Enter. The default location is /opt/SYMCScan.

7 When you are prompted whether you want Symantec Protection Engine to run as root, select one of the following settings:

   y Symantec Protection Engine is installed to run as root.

   n Symantec Protection Engine is installed not to run as root.

   Default setting.

8 If you selected not to run Symantec Protection Engine as root, type the user account that you want to use.

   The user account must already exist.
9 Press y to specify if you want to enable URL filtering and download URL definitions.

To change the setting after installation, go to Policies > Filtering > URL to enable this option.

For Core server only mode: See “Enabling URL filtering in the Core server only mode” on page 303.

10 Press y to specify if you want to enable URL Reputation and download URL Reputation definitions.

To change the setting after installation, go to Policies > Filtering > URL to enable this option.

For Core server only mode:

11 To specify whether you want to use the user-interface console in Symantec Protection Engine, select one of the following options:

y  Select this option if you want to use the user-interface console of Symantec Protection Engine.

Symantec Protection Engine automatically detects Java installed on your computer. If Java is not installed on your computer, you must specify the location where JRE 8.0 (update 121 or later) 64-bit is located

Proceed to step 12.

n  Select this option if you do not want to use the user-interface console of Symantec Protection Engine.

Proceed to step 15.

12 Select the port number on which the Web-based console listens.

The default port number is 8004. If you change the port number, use a number that is greater than 1024 that is not in use by any other program or service. You can disable the console by typing 0. If you disable the console, you can configure Symantec Protection Engine by editing the configuration data XML file.

See “About editing the Symantec Protection Engine configuration files” on page 365.
13 Specify the Secure Socket Layer (SSL) port number on which encrypted files are transmitted for increased security.

The default SSL port number is (8005). If this port is already in use, specify an SSL port that is not in use by any other program or service. Use a port number that is greater than 1024.

14 Type a password for the administrative account, and then confirm the password by typing it again.

15 Select the Insight Aggression Level from the following options:

- 1 for Low
- 2 for Medium
- 3 for High

The Insight aggression level defines how sensitive the Symantec Insight™ feature is to a file’s reputation score.

For Core server only mode: See “Configuring the Symantec Insight™ aggression level in the Core server only mode” on page 292.

The installer proceeds from this point with the installation.

See “About the Core server only mode” on page 249.

See “Symantec Protection Engine post-installation tasks” on page 61.

See “About installing Symantec Protection Engine” on page 35.

Upgrading Symantec Protection Engine on Linux

You can upgrade Symantec Protection Engine from a previous version to newer version. You can either preserve existing settings or uninstall previous version to install the newer version.

See “Configuring clean upgrade installation options on Linux” on page 57. to upgrade Symantec Protection Engine using the clean upgrade installation option.

See “Configuring preserve settings upgrade installation options on Linux” on page 59. to upgrade Symantec Protection Engine using the preserve settings upgrade installation option.

See “Installing Symantec Protection Engine on Linux” on page 53.

See “About installing Symantec Protection Engine” on page 35.
Configuring clean upgrade installation options on Linux

The clean upgrade option uninstalls the previous version of Symantec Protection Engine and installs the newer version.

To configure clean upgrade installation options on Linux

1. Log in to the computer on which you want to install Symantec Protection Engine as root.

2. Change directories to the location where the `SymantecProtectionEngine.sh` file is located in the product.zip file.
   `<drive>:\Symantec_Protection_Engine\RedHat\`

3. Type the following command:
   ```
   ./SymantecProtectionEngine.sh
   ```

4. Press `y` to continue with the interactive installation.

5. After you review with the Symantec License Agreement, press `y` to indicate that you agree with the terms of the agreement.
   If you indicate `n`, the installation is canceled.

6. Select 1 for the Clean upgrade option.
   Existing settings are not preserved.

7. Select the location to install Symantec Protection Engine, and then press `Enter`.
   The default location is `/opt/SYMCScan`.

8. When you are prompted whether you want Symantec Protection Engine to run as root, select one of the following settings:

   - **y**: Symantec Protection Engine is installed to run as root.
   - **n**: Symantec Protection Engine is installed not to run as root. Default setting.

9. If you selected not to run Symantec Protection Engine as root, type the user account that you want to use.
   The user account must already exist.
10 Press y to specify if you want to enable URL Filtering and download URL Filtering definitions.

To change the setting after installation, go to Policies > Filtering > URL to enable this option.

For Core server only mode: See “Enabling URL filtering in the Core server only mode” on page 303.

11 Press y to specify if you want to enable URL Reputation and download URL Reputation definitions.

To change the setting after installation, go to Policies > Filtering > URL to enable this option.

For Core server only mode:

12 To specify whether you want to use the user-interface console in Symantec Protection Engine, select one of the following options:

y Select this option if you want to use the user-interface console of Symantec Protection Engine.

Symantec Protection Engine automatically detects Java installed on your computer. If Java is not installed on your computer, you must specify the location where JRE 8.0 (update 121 or later) 64-bit is located.

Proceed to step 13.

n Select this option if you do not want to use the user-interface console of Symantec Protection Engine.

Proceed to step 16.

13 Specify the port number on which the Web-based console listens.

The default port number is 8004. If you change the port number, use a number that is greater than 1024 that is not in use by any other program or service. You can disable the console by typing 0. If you disable the console, you can configure Symantec Protection Engine by editing the configuration data XML file.

See “About editing the Symantec Protection Engine configuration files” on page 365.
14 Specify the Secure Socket Layer (SSL) port number on which encrypted files are transmitted for increased security.

The default SSL port number is (8005). If this port is already in use, specify an SSL port that is not in use by any other program or service. Use a port number that is greater than 1024.

15 Type a password for the administrator account, and then confirm the password by typing it again.

16 Select the Insight Aggression Level from the following options:
   - 1 for Low
   - 2 for Medium
   - 3 for High

   The Insight aggression level defines how sensitive the Symantec Insight™ feature is to a file’s reputation score.

   For Core server only mode:

   The installer proceeds from this point with the installation.

   See “Symantec Protection Engine post-installation tasks” on page 61.

See “Installing Symantec Protection Engine on Linux” on page 53.
See “Upgrading Symantec Protection Engine on Linux” on page 56.
See “About installing Symantec Protection Engine” on page 35.

Configuring preserve settings upgrade installation options on Linux

The preserved settings upgrade options uninstalls the existing version of Symantec Protection Engine and installs the version to which you want to upgrade Symantec Protection Engine.

If you are upgrading from version 5.x to version 7.x, you are required to type the virtual administrator account password due to introduction of stronger ciphers.

To configure Symantec Protection Engine with preserved settings upgrade installation options on Linux

1 Log in to the computer on which you want to install Symantec Protection Engine as root.

2 Change directories to the location where the SymantecProtectionEngine.sh file is located in the product.zip file.

   <drive>:\Symantec_Protection_Engine\RedHat\
3 Type the following command:

`. SymantecProtectionEngine.sh`

4 Press **y** to continue with the interactive installation.

5 After you review with the Symantec License Agreement, press **y** to indicate that you agree with the terms of the agreement. If you indicate **n**, the installation is canceled.

6 Select **2** for the Upgrade preserving existing settings option. Existing settings are preserved.

7 To specify whether you want to use the user-interface console in Symantec Protection Engine, select one of the following options:

   **y**  
   Select this option if you want to use the user-interface console of Symantec Protection Engine.
   Symantec Protection Engine automatically detects Java installed on your computer. If Java is not installed on your computer, you must specify the location where JRE 8.0 (update 121 or later) 64-bit is located.
   Proceed to step 8.

   **n**  
   Select this option if you do not want to use the user-interface console of Symantec Protection Engine.
   Proceed to step 10.

8 Specify the port number on which the Web-based console listens.

   The default port number is 8004. If you change the port number, use a number that is greater than 1024 that is not in use by any other program or service. You can disable the console by typing 0. If you disable the console, you can configure Symantec Protection Engine by editing the configuration data XML file.

   See “About editing the Symantec Protection Engine configuration files” on page 365.

9 Specify the Secure Socket Layer (SSL) port number on which encrypted files are transmitted for increased security.

   The default SSL port number is (8005). If this port is already in use, specify an SSL port that is not in use by any other program or service. Use a port number that is greater than 1024.

10 Type a password for the administrator account, and then confirm the password by typing it again.
Symantec Protection Engine post-installation tasks

The Symantec Protection Engine post-installation tasks are as follows:

- Verifying, stopping, and restarting the Symantec Protection Engine daemon on Linux
- Verifying, stopping, and restarting the Symantec Protection Engine service on Windows
- Clearing the Java cache
- About adding or changing authorized group name to access the Symantec Protection Engine console
- Accessing the Symantec Protection Engine console
- Enhancing security for the HTTPS servers and SSL servers
- Allocating resources for Symantec Protection Engine

Verifying, stopping, and restarting the Symantec Protection Engine daemon on Linux

Symantec Protection Engine starts automatically as a daemon when the installation is complete. A transcript of the installation is saved as /var/log/SYMCScan-install.log for later review. You can verify whether the service is running after you install the product.

You might need to stop and restart the Symantec Protection Engine daemon. When you do, the client applications that are submitting files for scanning can lose their connection to Symantec Protection Engine. The client applications must re-establish their connections and resubmit files for scanning.

Symantec Protection Engine also installs the new Symantec Protection Engine Update Manager service. Symantec Protection Engine LiveUpdate and Rapid Release requests are now served by this separate service. Symantec Protection Engine Update Manager service will be started and stopped by Symantec Protection Engine automatically.
To verify that the Symantec Protection Engine daemon is running on Linux

1. At the command prompt, type the following command:

   `ps -ea | grep symcscan`

   A list of processes similar to the following appears:

   ```
   5358  ? 0:00 symcscan
   5359  ? 0:00 symcscan
   ```

   If nothing is displayed, the Symantec Protection Engine daemon did not start.

2. If the Symantec Protection Engine daemon did not start, type the following command:

   `/etc/init.d/symcscan restart`

   With the new configuration, Symantec Protection Engine might take longer to start than it did in previous versions.

To stop and restart the Symantec Protection Engine daemon on Linux

1. Log in to the computer as root.

2. At the command prompt, type one of the following commands:

   To stop the service  `/etc/init.d/symcscan stop`

   To start the service `/etc/init.d/symcscan start`

   To stop and immediately restart the service

   `/etc/init.d/symcscan restart`

See “Clearing the Java cache” on page 64.

See “Accessing the Symantec Protection Engine console” on page 65.

Verifying, stopping, and restarting the Symantec Protection Engine service on Windows

Symantec Protection Engine starts automatically as a service when the installation is complete. You can verify whether the service is running after you install the product.

If the previous version runs under an account other than Local System account, then you can preserve the settings for logon credentials when you upgrade to the
newer version. You can type the service account password when you upgrade. However, if the password is incorrect, you can continue the upgrade but Symantec Protection Engine does not start automatically as a service. You must type the correct service account password and start the service manually.

You might need to stop and restart the Symantec Protection Engine service. When you do, the client applications that submit files to scan can lose their connection to Symantec Protection Engine. The client applications must reestablish their connections and resubmit files for scanning.

**Note:** Symantec Protection Engine might take longer to start than it did in versions before 5.0.

Symantec Protection Engine also installs the new Symantec Protection Engine Update Manager service. Symantec Protection Engine LiveUpdate and Rapid Release requests are now served by this separate service. Symantec Protection Engine Update Manager service will be started and stopped by Symantec Protection Engine automatically.

**To verify that the Symantec Protection Engine service is running on Windows**

1. In the Windows Control Panel, click **Administrative Tools**.
2. In the **Administrative Tools** window, click **Services**.
3. In the list of services, browse and locate **Symantec Protection Engine**.
4. Verify that the status indicates **Started**.

**To stop and restart the Symantec Protection Engine service on Windows**

1. In the Windows Control Panel, click **Administrative Tools**.
2. In the **Administrative Tools** window, click **Services**.
3. In the list of services, right-click **Symantec Protection Engine**, and do one of the following steps:

   - To stop the service: Click **Stop**.
   - To start the service: Click **Start**.
   - To stop and immediately restart the service: Click **Restart**.

See “Clearing the Java cache” on page 64.

See “Accessing the Symantec Protection Engine console” on page 65.
Clearing the Java cache

**Note:** This topic is applicable only when working in the Core server with user interface mode.

In some configurations, the caching of Java Applets might cause the Symantec Protection Engine console to display very slowly or fail to display at all. To prevent this problem, you must clear the Java cache and disable the caching feature.

**To clear the Java cache**

1. In the **Java Control Panel** dialog box, on the **General** tab, click **Settings**.
2. Clear the **Keep temporary files on my computer** check box.
3. Click **Delete Files**.
4. In the **Delete Temporary Files** dialog box, select the **Applications and Applets** and **Trace and Log Files** check boxes.
5. Click **OK**.

See “Accessing the Symantec Protection Engine console” on page 65.

About adding or changing authorized group name to access the Symantec Protection Engine console

**Note:** This topic is applicable only when working in the Core server with user interface mode.

If you proceed with installation without entering a valid domain\group for Windows Active Directory-based authentication, then Symantec Protection Engine service starts as usual. However, you cannot access the Symantec Protection Engine console. You must go to configuration.xml and enter the required information. You can update the domain\group information by using xml modifier. Ensure that you type a valid domain and security group. You must restart the Symantec Protection Engine service after making the change.

See “Add or change authorized group name to access Symantec Protection Engine console” on page 383.

See “Verifying, stopping, and restarting the Symantec Protection Engine service on Windows” on page 62.

See “Accessing the Symantec Protection Engine console” on page 65.
Accessing the Symantec Protection Engine console

Note: This topic is applicable only when working in the Core server with user interface mode.

The Symantec Protection Engine console is a Web-based interface that you can use to manage Symantec Protection Engine. The interface is provided through a built-in HTTPS server. You can access the interface by using the Windows Active Directory-based authentication or Symantec Protection Engine-based authentication. For Symantec Protection Engine-based authentication you can use the administrative account that you set up during installation. For Windows Active Directory-based authentication you can use your Windows Active Directory credentials to access the console. You access the Symantec Protection Engine console through a Web browser. You can use any computer on your network that can access the server that is running Symantec Protection Engine.

See “About the built-in HTTPS server” on page 67.

You do not need to restart Symantec Protection Engine after you modify a configuration setting for the changes to take effect. Most settings take effect when you apply them. If the Symantec Protection Engine service is restarted, connections to the client applications that are in the process of submitting files for scanning are lost. The client applications must re-establish their connections and resubmit files for scanning. You might want to schedule configuration changes for times when scanning is at a minimum.

The first time that you access the Symantec Protection Engine console after login, one of the following occurs:

The License page appears. No valid license is installed.

The License page is the only page that is active until you install a valid license.

The Home page appears. At least one valid license is installed.

You can navigate throughout the entire console.

Each time that you start a new browser session, log in, and open the console, the Home page appears.

Only one user should use the console at a time to avoid possible race conditions and configuration change conflicts.
To access the console with Symantec Protection Engine-based authentication

1. Launch a Web browser on any computer on your network that can access the server that is running Symantec Protection Engine.

2. In a Web browser, type the following address:
   
   \textbf{https://<servername>:<port>/}
   
   where \textit{<servername>} is the host name or IP address of the server that is running Symantec Protection Engine and \textit{<port>} is the port number that you selected during installation for the built-in Web server. The default port number is 8004.

3. If a \textbf{Security Alert} dialog box appears, click \textbf{Yes} to confirm that you trust the integrity of the applet, and then click \textbf{Yes} to display the Web page.

4. In the \textbf{Login Name} box, type a valid login name.

5. In the \textbf{Enter Password} box, type the password for the administrative account.

6. Press \textbf{Enter}.

   On successful login, Administrator is displayed on the upper right-hand side corner of the Symantec Protection Engine console.

To access the console with Windows Active Directory-based authentication

1. Launch a Web browser on any computer on your network that can access the server that is running Symantec Protection Engine.

2. In a Web browser, type the following address:
   
   \textbf{https://<servername>:<port>/}
   
   where \textit{<servername>} is the host name or IP address of the server that is running Symantec Protection Engine and \textit{<port>} is the port number that you selected during installation for the built-in Web server. The default port number is 8004.

3. If a \textbf{Security Alert} dialog box appears, click \textbf{Yes} to confirm that you trust the integrity of the applet, and then click \textbf{Yes} to display the Web page.

4. In the \textbf{Login Name} box, type a valid login name in the Domain\Username format.

5. In the \textbf{Password} box, type the password for your Windows Active Directory login name.

6. Press \textbf{Enter}.

   On successful login, the login name is displayed on the upper right-hand side corner of the Symantec Protection Engine console.

See “About authentication modes in Symantec Protection Engine” on page 36.
About the built-in HTTPS server

The built-in HTTPS server provides the console for Symantec Protection Engine. The built-in HTTPS server is independent of any existing HTTPS server that might be installed on your server. It is not a general-purpose Web server. During the installation process, you are prompted for the TCP/IP port number on which this built-in HTTPS server listens. The default setting is port 8004. If you specify a port number other than the default, remember which port number you chose. The port number that you specify must be exclusive to the Symantec Protection Engine console. Use a port number that is equal to or greater than 1024 and that is not already in use by another program or service. Do not use port number 443, which is the default port number for secure Web server connections.

You are also prompted upon installation to assign a Secure Socket Layer (SSL) port number on which encrypted files are transmitted for increased security. (The default port number is 8005.) If you change the port number, use a number that is equal to or greater than 1024. No other program or service should use the port number that you choose.

---

**Note:** When you configure your firewall, ensure that you do not block the ports for the built-in HTTPS server and the SSL.

---

See “Enhancing security for the HTTPS servers and SSL servers” on page 67.

See “Accessing the Symantec Protection Engine console” on page 65.

Enhancing security for the HTTPS servers and SSL servers

---

**Note:** This topic is applicable only when working in the Core server with user interface mode.

---

Symantec Protection Engine secures the HTTPS servers and SSL servers with public and private keys, which it creates when you install the product.

You can periodically force Symantec Protection Engine to generate new keys. You can also import keys from a third-party certificate.

See “Importing keys from a third-party certificate” on page 68.

See “Forcing Symantec Protection Engine to generate new keys” on page 69.
Importing keys from a third-party certificate

When you install Symantec Protection Engine, you also install a utility that you can use to import keys from third-party certificates. You must import the certificate file into a Java keystore format. You can import the certificate through a graphical user interface or at the command line. Symantec Protection Engine supports importing PFX and PKCS#12 certificate files.

See “Migrating to version 7.9” on page 86.

To import keys from a third-party certificate with the Certificate Import Utility graphical user interface

1. At the command line, change directories to the Symantec Protection Engine installation directory. The default installation directories are as follows:

   - Windows: C:\Program Files\Symantec\Scan Engine
   - Linux: /opt/SYMCscan/bin

2. Type the following to start the graphical user interface for the utility:

   java -jar certinstall.jar --gui

3. In the **Certificate Import Utility for Symantec Protection Engine 7.9** window, click **Load Certificate File**.

4. In the Load PFX/PKCS#12 Certificate File window, select the certificate file that you want to import.

5. In the **Enter password for certificate** window, type the password for the certificate.

   A text representation of the certificate appears.

6. Click **Import**.

7. In the **Select destination directory** window, select the directory to where you want to import the file.

   The keystore file that is created when you import the certificate is maintained in this directory. You must select the Symantec Protection Engine default installation directory.

8. Click **OK**.

   The file **keyStore.private** is created and placed in the destination directory.

9. Click **Exit** to close the Certificate Import Utility.
To import a third-party private key from the command line

1. At the command line, change directories to the Symantec Protection Engine installation directory. The default installation directories are as follows:

   Windows: `C:\Program Files\Symantec\Scan Engine`

   Linux: `/opt/SYMCScan/bin`

2. Do one of the following steps:

   To respond to command line prompts
   Type the following command:
   ```
   java -jar certinstall.jar --import
   ```
   You are prompted for responses. Type your response, and then press Enter.

   To specify the certificate file name and the destination directory in one command
   Type the following command:
   ```
   java -jar certinstall.jar --import --infile <PFX/PKCS12 certificate file name> --destination <SPE Dir>
   ```
   where `<PFX/PKCS12 certificate file name>` is the name of the certificate that you want to import, and `<SPE Dir>` is the Symantec Protection Engine installation directory.

To access the Certificate Import Utility help

◆ Do one of the following steps:

   In the Certificate Import Utility GUI
   On the menu bar, click Help.

   At the command line
   Type the following command:
   ```
   java -jar certinstall.jar --help
   ```

See "Forcing Symantec Protection Engine to generate new keys" on page 69.

Forcing Symantec Protection Engine to generate new keys

You should change the private key every two to five years to sustain long term security. You can force Symantec Protection Engine to generate new keys. When you delete the existing keystore, Symantec Protection Engine automatically creates new keys the next time you start the Symantec Protection Engine service.
To force Symantec Protection Engine to generate new keys

1. Stop the Symantec Protection Engine service.
2. In the installation directory, delete the following files:
   - keyStore.private
   - keyStore.public
3. Restart the Symantec Protection Engine service.

See “Verifying, stopping, and restarting the Symantec Protection Engine service on Windows” on page 62.

See “Verifying, stopping, and restarting the Symantec Protection Engine daemon on Linux” on page 61.

Changing the console settings

After installing Symantec Protection Engine, you can configure the console settings for Symantec Protection Engine.

Table 2-2 describes the console settings that you can configure.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Console server address</td>
<td>You manage Symantec Protection Engine through a Web-based interface, which is provided through a built-in HTTP server. The HTTP server binds to all interfaces by default. Specify the appropriate bind address to restrict administrative access.</td>
</tr>
<tr>
<td>Console port number</td>
<td>The Web-based interface binds to a TCP/IP port number. You are prompted to provide a port number during installation. You can change the port number through the console. If you change the port number, use a number that is equal to or greater than 1024. No other program or service should use the port number that you choose. <strong>Note:</strong> If you change the port number through the console, you must close and reopen the console. To access the console after the change, you must update the URL address to include the new port number.</td>
</tr>
</tbody>
</table>
Table 2-2  Console settings (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSL port number</td>
<td>Symantec Protection Engine uses a Secure Socket Layer (SSL) port to transmit files securely. You are prompted to provide an SSL port number during installation. You can change the port number through the console. If you change the SSL port number, use a number that is equal to or greater than 1024. No other program or service should use the port number that you choose. You must close and reopen the console for the new SSL port setting to take effect.</td>
</tr>
<tr>
<td>Console timeout</td>
<td>By default, Symantec Protection Engine is configured to automatically log off the user after a period of inactivity. The default period of inactivity is 300 seconds (five minutes). You can change the default timeout period. The minimum value is 60 seconds. <strong>Note:</strong> You must close and reopen the console for the new timeout interval setting to take effect.</td>
</tr>
</tbody>
</table>

To change the console settings

1. In the console on the primary navigation bar, click **System**.
2. In the sidebar under **Views**, click **Console Settings**.
3. In the content area under **Console Settings**, in the **Console server address** box, type a bind address, if necessary.
   
   By default, Symantec Protection Engine binds to all interfaces. Specify the appropriate bind address to restrict administrative access.
4. In the **Console port number** box, type a port number.
   
   The default setting is port 8004. If you change the port number, choose a port number that is exclusive to Symantec Protection Engine interface and that is greater than 1024. Do not use port number 80. To disable the console, type 0. If you disable the console, you must configure Symantec Protection Engine by editing the configuration file.
5 In the SSL port number box, type a secure port number.

The default setting is port 8005. If you change the port number, choose a port number that is exclusive to Symantec Protection Engine and that is between 1024 and 65535. Do not use port number 80 or port 443.

6 In the Console timeout box, type the period of inactivity, in seconds, after which the user is automatically logged off.

The default period of inactivity is 300 seconds (five minutes). The minimum value is 60 seconds; the maximum value is 3600 seconds (60 minutes).

7 On the toolbar, select one of the following options:

- **Save**
  
  Saves your changes.
  
  Use this option to continue making changes in the console until you are ready to apply them.

- **Apply**
  
  Applies your changes.
  
  Your changes are not implemented until you apply them.

You must close and reopen the console for the changes to the console settings to take effect.

See “About editing the Symantec Protection Engine configuration files” on page 365.

**Editing user information**

After installing Symantec Protection Engine, you can edit the user information for Symantec Protection Engine.

**Table 2-3** describes the user information that you can configure.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login name</td>
<td>Displays the login name for the user account.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: The login name cannot be edited.</td>
</tr>
<tr>
<td>Display name</td>
<td>Displays the display name for the user account.</td>
</tr>
</tbody>
</table>
Table 2-3  User information (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>New password</td>
<td>You can set a new password for the user account.</td>
</tr>
<tr>
<td></td>
<td>You cannot view the existing password of the user account.</td>
</tr>
<tr>
<td></td>
<td>See “About editing the Symantec Protection Engine configuration files” on page 365.</td>
</tr>
<tr>
<td>Confirm password</td>
<td>Type the password again to confirm it.</td>
</tr>
<tr>
<td>Email address</td>
<td>The existing email address (if any) is displayed.</td>
</tr>
<tr>
<td></td>
<td>The email address is an optional data field. You must type the email address in the <a href="mailto:name@symantecdomain.com">name@symantecdomain.com</a> format.</td>
</tr>
</tbody>
</table>

To edit the user information

1. In the console on the primary navigation bar, click **System**.
2. In the sidebar under **Views**, click **My Details**.
3. In the **Display name** box, type the new display name for the user account.
4. In the **New Password** box, type the new password for the user account.
5. Reconfirm the password by typing it again in the **Confirm password** box.
6. On the toolbar, select one of the following options:
   
   **Save** Saves your changes.
   
   Use this option to continue making changes in the console until you are ready to apply them.
   
   **Apply** Applies your changes.
   
   Your changes are not implemented until you apply them.

See “Managing user accounts” on page 73.

Managing user accounts

Multiple users can access the Symantec Protection Engine console and modify the configuration and policy of Symantec Protection Engine. To do so, the Administrator must first create user accounts with unique login names and passwords. Once you have a user account, access the Symantec Protection Engine console and sign in
with your login name and password. You can change the password after logging in to the console.

Note: The Administrator can create a maximum of 24 user accounts only. This number does not include the default Administrator user account.

See “Accessing the Symantec Protection Engine console” on page 65.

The Administrator is the user account created during a clean install. In case you do an upgrade of Symantec Protection Engine and preserve the existing settings, the existing user becomes the Administrator. You are recommended to remember the password for this account as it is the only account used to manage Symantec Protection Engine console users. If you want to change the password in the console, you must have the old password.

Note: Administrator can create, edit, or delete user accounts only for Symantec Protection Engine-based authentication.

The user login and logout information is logged when the logging level is set to Audit. With the multiple user account feature, you can monitor who logs in and logs out.

See “Logging levels and events” on page 202.

Note: Only the Administrator can create, edit, or delete user accounts. Hence, the Manage Users link is visible only to the Administrator.

See “Creating a new user account” on page 74.
See “Editing an existing user account” on page 76.
See “Deleting a user account” on page 78.
See “Viewing existing user accounts” on page 79.

Creating a new user account

Only the Administrator can access the Manage Users link to create a new user account. The Administrator can create a maximum of 24 user accounts only.

Table 2-4 describes the options that you must configure to create a new user.
### Table 2-4 Creating new user options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login name</td>
<td>Indicates the login name that you use to sign into the Symantec Protection Engine console. The login name must be unique and cannot be used for another user account. The length of the login name can be between 5 and 25 characters. The login name can contain any character except space characters. <strong>Note:</strong> The login name is not case-sensitive. <strong>Note:</strong> The login name field cannot be left blank.</td>
</tr>
<tr>
<td>Display name</td>
<td>Indicates the display name that you view on the top-right corner of the console after you log in with your user account credentials. The Display Name must not exceed 20 characters and is an optional data field. <strong>Note:</strong> The Display Name cannot be Administrator.</td>
</tr>
<tr>
<td>Password</td>
<td>Indicates the password that you use to sign into the Symantec Protection Engine console. The password field cannot be left blank.</td>
</tr>
<tr>
<td>Confirm password</td>
<td>Reconfirm the password by typing it again.</td>
</tr>
<tr>
<td>Email address</td>
<td>Indicates the email address of the user account. The email address is an optional data field. You must type the email address in the <a href="mailto:name@symantecdomain.com">name@symantecdomain.com</a> format. This parameter is optional.</td>
</tr>
</tbody>
</table>

**To create a new user account**

1. In the console on the primary navigation bar, click **System**.
2. In the sidebar under **Views**, click **Manage Users**.
   
   This link is visible only to those users who log into the Symantec Protection Engine console by using the Administrator account credentials.
3. In the content area under **Manage Users**, click the **Create new user** tab.
4 In the **Login name** box, type a unique login name.  
The login name must have a length between 5 and 25 characters.

5 In the **Display name** box, type a display name.  
This data field is optional.

6 In the **Password** field, type the password that the user must use to log in to the Symantec Protection Engine console.

7 Reconfirm the password by typing it again in the **Confirm password** box.

8 Type an email address for the user account in the **Email address** box.  
This parameter is optional.

9 On the toolbar, select one of the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Save</td>
<td>Saves your changes. Use this option to continue making changes in the console until you are ready to apply them.</td>
</tr>
<tr>
<td>Apply</td>
<td>Applies your changes. Your changes are not implemented until you apply them.</td>
</tr>
</tbody>
</table>

The information you type is lost if you click **Edit user** or **Delete user** tab without saving your entries.

See “Managing user accounts” on page 73.
See “Editing an existing user account” on page 76.
See “Deleting a user account” on page 78.
See “Viewing existing user accounts” on page 79.

**Editing an existing user account**

The Administrator can modify some parameters of existing user accounts.

**Table 2-5** describes the fields that the Administrator can edit in existing user accounts.
Table 2-5  Editing user account options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login name</td>
<td>Choose the login name of the user account that you want to modify from the drop-down menu.</td>
</tr>
<tr>
<td>Display name</td>
<td>The existing display name (if any) is shown here.</td>
</tr>
<tr>
<td>New password</td>
<td>You can set a new password for the user account.</td>
</tr>
<tr>
<td></td>
<td>You cannot view the existing password of the user account.</td>
</tr>
<tr>
<td>Confirm</td>
<td>Reconfirm the new password by typing it again.</td>
</tr>
<tr>
<td>Email address</td>
<td>The existing email address (if any) is displayed.</td>
</tr>
<tr>
<td></td>
<td>This parameter is optional.</td>
</tr>
</tbody>
</table>

To edit an existing user account

1. In the console on the primary navigation bar, click **System**.
2. In the sidebar under **Views**, click **Manage Users**.
   This link is visible only to those users who log into the Symantec Protection Engine console by using the Administrator account credentials.
3. In the content area under **Manage Users**, click the **Edit user** tab.
4. Select the user account that you want to edit from the drop-down box in Login name.
5. Edit the user account display name in the **Display name** box.
6. In the **New password** box, type the new password that the user must use to log in to the Symantec Protection Engine console.
   The password field cannot be left blank.
7. Reconfirm the password by typing it again in the **Confirm** box.
8 Edit the user account email address in the Email address box.
   This parameter is optional.

9 On the toolbar, select one of the following options:

   Save                      Saves your changes.
   - Use this option to continue making changes in the console until you are ready to apply them.

   Apply                     Applies your changes.
   - Your changes are not implemented until you apply them.

   The information you type is lost if you click Create new user or Delete user tab without saving your entries.

   See "Managing user accounts" on page 73.
   See "Creating a new user account" on page 74.
   See "Deleting a user account" on page 78.
   See “Viewing existing user accounts” on page 79.

Deleting a user account

In addition to creating and editing user accounts, the Administrator can delete existing user accounts in Symantec Protection Engine.

Table 2-6 describes the fields that the Administrator must configure to delete a user account.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login name</td>
<td>Displays the login names of all existing user accounts.</td>
</tr>
<tr>
<td>Delete</td>
<td>To delete a specific user account, put a check mark against the user account.</td>
</tr>
</tbody>
</table>
To delete a user account

1. In the console on the primary navigation bar, click System.
2. In the sidebar under Views, click Manage Users.
   This link is visible only to those users who log into the Symantec Protection Engine console by using the Administrator account credentials.
3. In the content area under Manage Users, click the Delete user tab.
4. To delete a particular user account, put a check mark in the Delete column corresponding to the user account.
5. On the toolbar, select one of the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Save</td>
<td>Saves your changes. Use this option to continue making changes in the console until you are ready to apply them.</td>
</tr>
<tr>
<td>Apply</td>
<td>Applies your changes. Your changes are not implemented until you apply them.</td>
</tr>
</tbody>
</table>

The information you type is lost if you click Create new user or Edit user tab without saving your entries.

See “Managing user accounts” on page 73.
See “Creating a new user account” on page 74.
See “Editing an existing user account” on page 76.
See “Viewing existing user accounts” on page 79.

Viewing existing user accounts

You can view existing user accounts on the Symantec Protection Engine by using the Administrator account credentials. All user accounts except the Administrator user account are visible under the Manage Users link. The existing users list is empty when you log into Symantec Protection Engine for the first time.

Table 2-7 describes the existing user account details that you can view.
### Table 2-7: Visible details of existing user accounts

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login name</td>
<td>Displays the unique login name of the user account that the user must use to log into the Symantec Protection Engine console.</td>
</tr>
<tr>
<td>Display name</td>
<td>Displays the user account display name that is visible on the top-right corner of the console once the user logs in.</td>
</tr>
<tr>
<td>Email address</td>
<td>Displays the email address for the user account. This parameter is optional.</td>
</tr>
</tbody>
</table>

#### To view existing user accounts

1. In the console on the primary navigation bar, click **System**.
2. In the sidebar under **Views**, click **Manage Users**.
   - This link is visible only to those users who log into the Symantec Protection Engine console by using the Administrator account credentials.
3. In the content area under **Existing Users**, you can view existing user accounts on the Symantec Protection Engine.

   - See “Managing user accounts” on page 73.
   - See “Creating a new user account” on page 74.
   - See “Editing an existing user account” on page 76.
   - See “Deleting a user account” on page 78.

#### About security notice

You can configure Symantec Protection Engine to display a custom security notice to all users before they log in. You can use this feature to ensure that users view common security information before they log in to the Symantec Protection Engine console.

- See “Enabling security notice feature” on page 80.

#### Enabling security notice feature

The security notice feature can be accessed using any user account credentials in the Symantec Protection Engine console.
To enable the security notice feature

1. In the console on the primary navigation bar, click System.
2. In the sidebar under Views, click Security Notice.
3. In the content area under Security Notice, check the Display security notice option.
   To disable the feature, uncheck the option.
4. Type the text that you want all users to view before logging in the Security Notice Content text box.
   You can type up to a maximum of 1500 characters in the Security Notice Content text box.
5. On the toolbar, select one of the following options:

   Save: Saves your changes.
   Use this option to continue making changes in the console until you are ready to apply them.

   Apply: Applies your changes.
   Your changes are not implemented until you apply them.

6. Close the existing Symantec Protection Engine console and access the console once again for changes to take effect.

See “About security notice” on page 80.

Allocating resources for Symantec Protection Engine

You can allocate resources for Symantec Protection Engine and limit the system resources that are devoted to scanning. You can also limit the server resources that Symantec Protection Engine uses for processing files in memory.

Table 2-8 describes the resource settings.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Temporary directory for scanning | Symantec Protection Engine stores files in the installation directory temporary folder for scanning. You can change the location of this temporary directory to support sites with large, specialized disk configurations. The disk space that is required for this directory varies depending on the volume of data to be scanned. Symantec Protection Engine performance depends on this directory being able to accommodate a large volume of data during periods of peak use. If you want to change the temporary directory location, ensure that it has the proper access permissions so that only authorized entity can access it. The file directory that you specify must already exist. Symantec Protection Engine validates the existence of the directory when you save or apply your changes. The default temporary directories are as follows:  
  - Linux: `<Installdir>/temp`  
  - Windows: `<Installdir>	emp`                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Number of available threads for scanning | You can specify the maximum number of threads that are available for scanning. The pool of threads that is available to Symantec Protection Engine for scanning dynamically adjusts to the load that is being processed. You can change a number of additional related parameters in the configuration file. The optimal settings for these parameters vary depending on your environment and how you use Symantec Protection Engine. Symantec Protection Engine performance depends on the following:  
  - Volume of data being scanned  
  - Number of the client applications that make requests  
  - Available memory and disk space  
  - Number of scanning threads  
See “Control the dynamic thread pool” on page 369.  
**Note:** If you use the RPC protocol and support multiple RPC clients, Symantec Protection Engine creates a separate pool of threads for each RPC client. (The RPC clients do not share a common pool of threads.) The number of available threads for scanning that you select for this setting is applied to each RPC client individually.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Threshold number of queued requests | Symantec Protection Engine is at maximum load when the number of queued requests exceeds the specified threshold. You can configure Symantec Protection Engine to log the event to the specified logging destinations when the queue exceeds the maximum load. See "Logging levels and events" on page 202. When the ICAP threshold notification feature is enabled (default value), Symantec Protection Engine takes the following actions:  
  - Logs the event to the logging destinations  
  - Rejects the scan request  
  - Notifies the client that the server is too busy to process the request  
When the ICAP threshold notification feature is disabled, Symantec Protection Engine continues to queue all incoming requests after the threshold is exceeded until a thread becomes available. You can configure the threshold for queued requests for Symantec Protection Engine. The client can then adjust the load balancing, which prevents the server from being overloaded with scan requests.  
**Note:** For logging to occur at maximum load, the logging level for the logging destination must be set to Warning or higher. |
Symantec Protection Engine generates log entries and alerts at a prescribed interval to notify you that it is at the maximum threshold for scan requests. The alert interval is the number of minutes between each log entry or alert. The default interval is every five minutes. If you change the interval, select one that is informative but does not result in an excessive number of log entries or alerts.

You receive an SMTP alert every \( n \) minutes when Symantec Protection Engine rejects a scan request because it is too busy when all of the following conditions are met:

- You use ICAP.
- The ICAP threshold client notification feature is enabled (default setting).
- You enable SMTP alerts.
- You configure "Log or send alert for maximum load every \( n \) minutes."

Symantec Protection Engine posts log entries and sends SNMP alerts for each event in which a scan request is rejected because the server is too busy.

See “Activating SMTP alerts” on page 214.

Symantec Protection Engine can decompose and scan the contents of container files in memory, which eliminates the latency imposed by on-disk scanning. This feature can improve performance in environments in which large volumes of container and archive file formats are routinely submitted for scanning. You can limit the resources that are consumed for processing files in memory by specifying the following values:

- The maximum RAM to use for the in-memory file system (in megabytes)
- The maximum file size that can be stored within the in-memory file system (in megabytes)

To allocate resources for Symantec Protection Engine

1. In the console on the primary navigation bar, click **Configuration**.
2. In the sidebar under **Views**, click **Resources**.
3. In the content area under **System Scanning Resources**, in the **Temporary directory for scanning** box, type the temporary directory to be used for scanning.

To prevent scanning conflicts between Symantec Protection Engine and any other client antivirus software installed on the server, make sure that the client antivirus software avoids all scans of the Symantec Protection Engine temporary directory (for example, real-time scans, manual scans, and scheduled scans).

4. In the **Number of available threads for scanning** box, type the maximum number of scanning threads that are allowed for scanning.

   The default settings depend on the number of cores of the processor.

   See “About available threads for scanning” on page 165.

5. In the **Threshold number of queued requests** box, type the threshold number of queued requests that Symantec Protection Engine considers to be at maximum load.

   The default setting is 100.

6. In the **Log or send alert for maximum load every ___ minutes** box, type the alert interval in minutes.

   The default setting is 5 minutes.

7. Under **Server Resources**, in the **Maximum RAM used for in-memory file system** box, type the maximum amount of RAM that can be used for the in-memory file system.

   The default setting is 2048 MB. The maximum value is 4096 MB (4 GB).

8. In the **Maximum file size stored within the in-memory file system** box, type the maximum file size that can be stored in the in-memory file system.

   The default setting is 256 MB. The maximum setting is 2048 MB (2 GB). Files that exceed the specified size are written to the disk.

9. On the toolbar, select one of the following:

   - **Save**: Saves your changes.
     - This option lets you continue making changes in the console until you are ready to apply them.

   - **Apply**: Applies your changes.
     - Your changes are not implemented until you apply them. You must perform a manual restart for the changes to take effect.
Migrating to version 7.9

Table 2-9 describes the upgrades that Symantec Protection Engine supports.

<table>
<thead>
<tr>
<th>Previous version number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.8.x</td>
<td>Symantec Protection Engine 7.9 supports an upgrade from version 7.8.x. You can choose to upgrade the product and preserve your existing settings or perform a clean upgrade. If you choose to do a clean upgrade, the installer removes the previous version, and then installs the newer version as a full installation, without preserving any previous settings.</td>
</tr>
<tr>
<td>7.5.x</td>
<td>Symantec Protection Engine does not support direct upgrades from version 7.5.x. You must first migrate to version 7.8.0. A separate utility to migrate from 7.5.x to 7.8.0 is provided. For more information, see the Symantec Protection Engine 7.8.0 Migration Utility at the following location: <a href="https://support.symantec.com/en_US/article.INFO3603.html">https://support.symantec.com/en_US/article.INFO3603.html</a></td>
</tr>
<tr>
<td>7.0.x</td>
<td>Symantec Protection Engine does not support direct upgrades from version 7.0.x. You must first upgrade to version 7.5.x.</td>
</tr>
<tr>
<td>5.1/5.2</td>
<td>Symantec Protection Engine does not support direct upgrades from version 5.1 or 5.2. You must first upgrade to version 7.0.x.</td>
</tr>
</tbody>
</table>

You must stop the Symantec Protection Engine service before you upgrade the software.

See “Verifying, stopping, and restarting the Symantec Protection Engine service on Windows” on page 62.

See "Importing keys from a third-party certificate" on page 68.

About retaining the service account when you upgrade to version 7.9

On Windows platforms, if the previous version runs under an account other than the Local System account, then you can preserve the service logon credentials. During the upgrade, Symantec Protection Engine automatically populates the service account name (non-editable) in the Symantec Protection Engine Service Credentials screen. You can then enter the password for this service account. If the password is incorrect, you can continue the upgrade but the Symantec Protection
Engine service does not start. Once the installation is complete, you must type the correct service account password and start the service manually.

---

**Note:** The *Symantec Protection Engine Service Credentials* screen appears only if the previous version of Symantec Protection Engine runs on the account other than Local System.

See “About installing Symantec Protection Engine” on page 35.

See “Upgrading Symantec Protection Engine on Windows” on page 43.

---

## Uninstalling Symantec Protection Engine

When you uninstall Symantec Protection Engine, the license keys remain. If you want to permanently uninstall Symantec Protection Engine, you must manually uninstall the license keys.

See “About removing license files” on page 93.

When you uninstall Symantec Protection Engine, the keystore files also remain, which eliminates the need to re-import certificates if you uninstall and reinstall the product.

See “Enhancing security for the HTTPS servers and SSL servers” on page 67.

### To uninstall Symantec Protection Engine on Windows

1. Log on to the computer as administrator or as a user with administrator rights.

2. In the **Add or Remove Programs Control Panel**, click **Symantec Protection Engine**.

3. Click **Remove**.

4. Follow the instructions to complete the uninstallation.

### To uninstall Symantec Protection Engine on Linux

1. Log in to the computer as root.

2. At the command prompt, type the following command:

   ```
   rpm -e SYMCScan
   ```
Activating licenses

This chapter includes the following topics:

- About licensing
- About license activation

About licensing

You activate key features for Symantec Protection Engine when you install the appropriate license. Key features include scanning for threats and security risks, HTTP content filtering, and related updates. You must install the licenses through the Symantec Protection Engine console.

For complete scanning functionality and definition updates, you need the following licenses:

<table>
<thead>
<tr>
<th>Product licenses</th>
<th>Product licenses activate scanning functionality.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The AV Scanning license activates the threat scanning features and security risk scanning features. The URLFiltering license activates the HTTP URL filtering features. URL Reputation license activates URL Reputation feature.</td>
</tr>
<tr>
<td></td>
<td>See “About scanning for risks” on page 110.</td>
</tr>
<tr>
<td></td>
<td>See “About categories” on page 168.</td>
</tr>
</tbody>
</table>
### Content licenses

Content licenses let you receive product updates. The AV Content license lets you receive updated threat and security risk definitions. Updated definitions ensure that your server is protected from risks.

The URL Content license lets you receive updated Content Category lists.

The URL Reputation Content license lets you use updated IP, Domain/URL Reputation feeds.

See “About definition updates” on page 226.

### Symantec Insight™ license

Symantec Insight™ license activates the Insight scanning and the Insight revocation feed update functionality.

See “About Symantec Insight™” on page 139.

### Symantec APK Reputation license

Symantec APK Reputation license activates the APK Reputation functionality.

---

You must have valid product licenses to configure the product and to access the threat (antivirus) scanning, security risk scanning, and HTTP content filtering features. Without valid product licenses, you cannot access these features in the console.

The first time that you open the console after installation, only the License view is active. You must install the AV Scanning license to access the Configuration, Reports, Monitors, and System pages in the console. You must have the AV Scanning and URL Filtering licenses installed to access the Policies pages. You must also activate the Insight license to take advantage of the Insight scanning feature.

---

**Note:** If you upgrade from a previous version and your licenses are current, Symantec Protection Engine automatically recognizes these licenses. You do not need to reinstall your licenses.

Symantec Protection Engine installs with the most current definitions that are available at the time the product is released. After you install the product and activate the licenses, perform a definition update to obtain the most current definitions. If you discover a problem with the new definitions, revert to the definitions that were shipped with the product.

See “Rolling back definitions” on page 245.

When a license is within 60 days of its expiration date, it is considered to be in a warning period. After a license expires with no license renewal, all record of the
license is removed. To regain product functionality, you must renew and reactivate your license subscription.

You can configure Symantec Protection Engine to generate log entries when a license is in the warning period.

See “About logging data” on page 200.

See “Checking the license status” on page 93.

About license activation

You activate scanning features and definitions updates for Symantec Protection Engine with licenses. A separate license must be installed for each feature. If you purchase additional product features from Symantec as they become available for Symantec Protection Engine, these features require a new license.

Symantec issues a serial number for each type of license that you purchase. This serial number is required to register your product and your maintenance agreement. The serial number is provided on a license certificate, which is mailed separately and arrives in the same time frame as your software. For security reasons, the license certificate is not included in the Symantec Protection Engine software distribution package. If you upgrade from a previous version and you have an active maintenance contract, you might receive the serial number certificate with an upgrade insurance letter.

See “If you do not have a serial number” on page 90.

License activation involves the following process:

**Obtain a license file from Symantec.**

To request a license file, you must have the license serial number for each license that you want to activate. After you complete the registration process, Symantec sends you the appropriate license file by email.

See “Obtaining a license file” on page 91.

**Install the license file.**

You must install the content licenses and product licenses on each server on which you run Symantec Protection Engine. When you install the licenses, you can enable the scanning processes and update your product and its associated content.

See “Installing the license file” on page 92.

If you do not have a serial number

Your license certificate contains the serial numbers for the license that you purchase. The license certificate should arrive within three to five business days of when you
receive your software. If you do not receive the license certificate, contact Symantec Customer Service at 800-721-3934 or your reseller to check the status of your order. If you have lost your license certificate, contact Symantec License Administration.

See “Where to get more information” on page 28.

Obtaining a license file

Each license certificate or upgrade certificate has a serial number. The serial number is used to request a license file and to register for support. To request a license file, you must have the serial number for the license.

The serial number is printed on the license certificate or upgrade certificate that Symantec mails to you. The format of a serial number is a letter followed by 10 digits. For example, F2430482013.

If you purchase multiple types of licenses but register them separately, Symantec sends you a separate license file for each license. You must install each license file separately. If you register multiple licenses at the same time, Symantec sends you a single license file that contains all of your licenses.

The license file that Symantec sends to you is contained within a .zip file. The .slf file that is contained within the .zip file is the actual license file. Ensure that your inbound email environment permits .zip email message attachments.

---

Warning: License files are digitally signed. If you try to edit a license file, you render it invalid.

---

To obtain a license file

1 In a Web browser, type the following address:
   
   https://licensing.symantec.com

   Your Web browser must use 128-bit encryption to view the site.

2 If a Security Alert dialog box appears, click OK.

3 Follow the procedures on the Symantec Licensing Portal to register your license and request your license file.

   Symantec sends you an email message that contains the license file in an attachment. If the email message does not arrive within two hours, an error might have occurred. Try again to obtain the license file through the Symantec Web site. If the problem continues, contact Symantec Technical Support.

   See “Where to get more information” on page 28.
Installing the license file

A license file contains the information that is required to activate one or more features in a product. A license file is also required to update the product and its associated content. A license file might contain one or more types of licenses. The number of licenses it contains depends on whether you registered the license serial numbers separately or at the same time.

See “Obtaining a license file” on page 91.

You can install the license file through the console. If you disabled the console, you can install the license file by copying it to a specific directory location.

**Note:** You must restart Symantec Protection Engine manually after saving the license files.

To install the license file through the console

1. When you receive the email message from Symantec that contains the license file, save the file that is attached to the email message to the computer from which you intend to access the Symantec Protection Engine console.

2. In the console on the primary navigation bar, click System. If no license has been installed, when you open the console, the System tab appears by default.

3. In the sidebar under Views, click License.

4. Under Tasks, click Install License.

5. In the Install License window, click Browse.

6. In the Load File window, browse to the folder location where you saved the license file, select it, and then click Open.

7. In the Install License window, click Install.

A status message indicates that the license was successfully installed.

To install the license file without using the console:

- Based on the operating system, save the license file that you receive in an email message from Symantec in the following location:

  - **Windows**: C:\ProgramData\Symantec Shared\Licenses
  - **Linux**: /opt/Symantec/Licenses
About removing license files

The license files for Symantec Protection Engine are not uninstalled automatically if you uninstall the product. The license files remain in place so that if you need to reinstall the product, the license remains intact. Each license that is installed is stored in a separate file in the shared license directory. This shared directory contains the licenses for all Symantec products. The license files must be removed manually.

The default license directories are as follows:

- **Windows**: `C:\ProgramData\Symantec Shared\Licenses`
- **Linux**: `/opt/Symantec/Licenses`

See “About licensing” on page 88.

Checking the license status

You can view information about the status of your Symantec Protection Engine licenses. You can check the license expiration date and the number of days that remain in the warning period.

Table 3-1 describes the license information that is displayed on the License page.

<table>
<thead>
<tr>
<th>Table 3-1</th>
<th>License status information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Column</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>Feature</td>
<td>This column lists each license that is installed.</td>
</tr>
<tr>
<td>Expiration</td>
<td>This column lists the expiration date for each license. If the license is in the warning period, a warning message is displayed in this column.</td>
</tr>
<tr>
<td>Fulfillment ID</td>
<td>The fulfillment ID is the identification number for your license. You must provide this number to Symantec customer care if you have questions about your license.</td>
</tr>
</tbody>
</table>

The Quick Status pane on the Home page also displays the licenses that are installed. When a license is about to expire, the License page displays the warning.

To check the license status

1. In the console on the primary navigation bar, click **System**.
2. In the sidebar under **Views**, click **License**.

   The licensing information appears in the content area.

See “About licensing” on page 88.
Configuring scanning services for client applications

This chapter includes the following topics:

- About the communication protocols
- About working with ICAP
- About working with the RPC protocol
- Editing the service startup properties

About the communication protocols

You can select the communication protocol that Symantec Protection Engine uses to communicate with the client applications for which it provides scanning services. You must configure protocol-specific configuration options, which differ depending on the protocol that you select.

You can choose from the following protocols:

- Internet Content Adaptation Protocol (ICAP)
  - Symantec Protection Engine uses ICAP by default. ICAP is a lightweight protocol for executing a remote procedure call on HTTP messages. Symantec Protection Engine supports version 1.0 of ICAP, as presented in RFC 3507 (April 2003).
  - See “About working with ICAP” on page 97.

- Remote Procedure Call (RPC)
  - See “About working with the RPC protocol” on page 100.
Supported services by protocol

The services that are available through Symantec Protection Engine differ depending on the protocol that you use.

Table 4-1 lists the services that are available for each protocol.

**Table 4-1 Supported services by protocol**

<table>
<thead>
<tr>
<th>Feature</th>
<th>ICAP</th>
<th>RPC protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat detection</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>See “Enabling threat detection in Symantec Protection Engine” on page 114.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security risk detection</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>See “Enabling nonviral threat detection in Symantec Protection Engine” on page 117.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Insight detection</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>See “About Symantec Insight™” on page 139.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>APK Reputation detection</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>See “About Android Application (APK) Reputation” on page 193.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>URL Reputation detection</td>
<td>Supported</td>
<td>Not Supported</td>
</tr>
<tr>
<td>See “About URL Reputation” on page 191.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Container processing limits</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>See “Setting container file limits” on page 161.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Partial and encrypted malformed MIME detection</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>See “About container files in Symantec Protection Engine” on page 130.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>File name filtering</td>
<td>Supported</td>
<td>N/A</td>
</tr>
<tr>
<td>See “Configuring file name filtering in Symantec Protection Engine” on page 122.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>File or attachment size filtering</td>
<td>Supported</td>
<td>N/A</td>
</tr>
<tr>
<td>See “Configuring file size filtering in Symantec Protection Engine” on page 124.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Feature</td>
<td>ICAP</td>
<td>RPC protocol</td>
</tr>
<tr>
<td>--------------------------------------------------------------</td>
<td>----------</td>
<td>--------------</td>
</tr>
<tr>
<td>Scanning by file extension and file type</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>See “Specifying which files to scan” on page 157.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Scanning by file size</td>
<td>Supported</td>
<td>N/A</td>
</tr>
<tr>
<td>See “Specifying the maximum file or message size to scan” on</td>
<td></td>
<td></td>
</tr>
<tr>
<td>page 160.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Message origin filtering</td>
<td>Supported</td>
<td>N/A</td>
</tr>
<tr>
<td>See “Configuring message origin filtering in Symantec</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Protection Engine” on page 128.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Subject line content filtering</td>
<td>Supported</td>
<td>N/A</td>
</tr>
<tr>
<td>See “Configuring subject line content filtering in Symantec</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Protection Engine” on page 126.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Quarantining infected files</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>See “About quarantining files in Symantec Protection Engine”</td>
<td></td>
<td></td>
</tr>
<tr>
<td>“ ” on page 119.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HTTP content filtering</td>
<td>Supported</td>
<td>N/A</td>
</tr>
<tr>
<td>See “How to filter a URL” on page 182.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Logging events to the following destinations:</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>■ Local logs</td>
<td></td>
<td></td>
</tr>
<tr>
<td>See “About configuring local logging” on page 207.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>■ Windows Application Event Log</td>
<td></td>
<td></td>
</tr>
<tr>
<td>See “Configuring logging to the Windows Application Event</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Log” on page 212.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>■ Statistics Log</td>
<td></td>
<td></td>
</tr>
<tr>
<td>See “Enabling statistics reporting in Symantec Protection</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Engine” on page 211.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>■ Abort log</td>
<td></td>
<td></td>
</tr>
<tr>
<td>See “Logging destinations” on page 200.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>■ Linux Syslog</td>
<td></td>
<td></td>
</tr>
<tr>
<td>See “Configuring logging to the Linux Syslog” on page 213.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 4-1  Supported services by protocol (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>ICAP</th>
<th>RPC protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>RPC client logging</td>
<td>N/A</td>
<td>Supported</td>
</tr>
<tr>
<td>See “Logging to the RPC client logging subsystem” on page 107.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Monitor scanning requests</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>See “Monitoring scanning requests” on page 146.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Continuous self-test scanning</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>See “Disable automatic self-test scanning” on page 379.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Notification to the client that the queued requests threshold is reached</td>
<td>Supported</td>
<td>Supported (For Cluster mode only)</td>
</tr>
<tr>
<td>See “Allocating resources for Symantec Protection Engine” on page 81.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>See “Disable the ICAP threshold client notification” on page 372.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SMTP and SNMP alert and outbreak notifications</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>See “About configuring alerts” on page 213.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Command-line scanning</td>
<td>Supported</td>
<td>N/A</td>
</tr>
<tr>
<td>See “About the Symantec Protection Engine command-line scanner” on page 337.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

About working with ICAP

In its default configuration, Symantec Protection Engine uses ICAP to communicate with the clients that run ICAP version 1.0, as presented in RFC 3507 (April 2003). Any client that uses this standard can use ICAP to communicate with Symantec Protection Engine to request scanning services.

The Symantec Protection Engine software development kit (SDK) is available for developing custom integrations with version 1.0 of ICAP. It includes client-side application program interfaces (API) to simplify the addition of AV scanning to any C, C++, Java, or .Net application.

When you use ICAP as the communication protocol, Symantec Protection Engine initially provides information to the ICAP client about which file types to scan. This information is based on the configuration of Symantec Protection Engine.
If the file extension is one that is identified for scanning, the ICAP client forwards the entire file to Symantec Protection Engine. If the file extension is unknown or is not one that is identified for scanning, the ICAP client forwards the first few bytes of the file. Symantec Protection Engine examines the first few bytes of the file to determine whether the file might contain a threat or security risk. Based on this examination, Symantec Protection Engine might request and scan a file even when it is not identified for scanning.

Symantec Protection Engine also scans POST transactions (sending data from a Web browser to a server using the HTTP protocol). When a threat or security risk is detected in a POST transaction file, Symantec Protection Engine blocks the file without trying to repair it. An HTTP message informs the posting client that a risk was detected and that the file was blocked.

**Configuring ICAP options**

If you select ICAP, you must configure certain options specific to ICAP protocol. You must also configure the ICAP client to work with Symantec Protection Engine. For more information, see the ICAP client documentation.

See “Configuring ICAP options in the Core server only mode” on page 255.

Table 4-2 describes the configuration options for ICAP.
Table 4-2  Protocol-specific options for ICAP

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bind address</td>
<td>Symantec Protection Engine detects all of the available IP addresses that are installed on the host. By default, Symantec Protection Engine accepts scanning requests on (binds to) all of the scanning IP addresses that it detects. You can configure up to 64 IP addresses as scanning IP addresses. You can specify whether you want Symantec Protection Engine to bind to all of the IP addresses that it detects, or you can restrict access to one or more interfaces. If you do not specify at least one IP address, Symantec Protection Engine binds to all of the scanning IP addresses that it detects. If Symantec Protection Engine fails to bind to any of the selected IP addresses, an event is written to the log as a critical error. Even if Symantec Protection Engine is unable to bind to any IP address, you can access the console. However, scanning functionality is unavailable. See “Logging levels and events” on page 202. Note: You can use 127.0.0.1 (the loopback interface) to let only the clients that are running on the same computer connect to Symantec Protection Engine.</td>
</tr>
<tr>
<td>Port number</td>
<td>The port number must be exclusive to Symantec Protection Engine. You must use the same port number for all of the scanning IP addresses that you want to bind to Symantec Protection Engine. The default port number is 1344. If you change the port number, use a number that is equal to or greater than 1024. No other program or service should use this port number.</td>
</tr>
</tbody>
</table>

To configure ICAP options

1. In the console on the primary navigation bar, click Configuration.
2. In the sidebar under Views, click Protocol.
3. In the content area under Select Communication Protocol, click ICAP.
4. In the Manual Restart Required dialog box, click OK.

Whenever you switch protocols, you must restart the server. You can continue to make and apply changes in the console. However, the changes do not take effect until you restart the Symantec Protection Engine service.
5 Under **ICAP Configuration**, in the Bind address table, select the scanning IP addresses that you want to bind to Symantec Protection Engine. Check **Select All** to select every IP Address in the Bind address table.

Only four IP addresses appear in the Bind address table. Click the scroll bar to view additional IP addresses.

By default, Symantec Protection Engine binds to all interfaces.

6 In the **Port number** box, type the TCP/IP port number that the client application uses to pass files to Symantec Protection Engine for scanning.

The default setting for ICAP is port 1344. If you change the port number, use a number that is equal to or greater than 1024. No other program or service should use this port number. You must use the same port number for every scanning IP addresses that you want to bind to Symantec Protection Engine.

7 On the toolbar, select one of the following options:

- **Save** Saves your changes.
  
  Use this option to continue making changes in the console until you are ready to apply them.

- **Apply** Applies your changes.
  
  Your changes are not implemented until you apply them.

See “About working with ICAP” on page 97.

See “Verifying, stopping, and restarting the Symantec Protection Engine service on Windows” on page 62.

### About working with the RPC protocol

You can configure Symantec Protection Engine to use the RPC protocol to interface with appropriate clients. To use the RPC protocol, Symantec Protection Engine must be installed on a computer that is running Windows 2008 Server, Windows 2012 Server, or Windows 2016 Server. It must also be located in the same domain as the RPC clients for which it provides scanning and repair services. A single protection engine can support multiple RPC clients. For sites with larger scan volumes, multiple protection engines also can be used to support one or more RPC clients.

A connection is maintained between each RPC client and Symantec Protection Engine. Symantec Protection Engine monitors the connection with each RPC client by checking the connection at a configured time interval. If Symantec Protection Engine determines that the connection is not active, it tries to reconnect. (You can
configure the number of times that Symantec Protection Engine tries to reestablish the connection.) Symantec Protection Engine stops checking the connection with the RPC client when it reaches the maximum number of tries. Symantec Protection Engine resumes trying connections when the protection engine service restarts.

See “Verifying, stopping, and restarting the Symantec Protection Engine service on Windows” on page 62.

About RPC configuration options

If you select RPC as the protocol, configure certain RPC-specific settings and the RPC client to work with Symantec Protection Engine. You must also restart the Symantec Protection Engine service for the RPC protocol to take effect.

Table 4-3 describes the configuration options for RPC.

<table>
<thead>
<tr>
<th>Table 4-3</th>
<th>Protocol-specific options for RPC</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Option</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>RPC client list</td>
<td>A single Symantec Protection Engine can support multiple RPC clients. Clients must be located in the same domain as Symantec Protection Engine. You must provide the IP address of each RPC client. Enter 127.0.0.1 in RPC client list to be able to operate in the Cluster mode. See “Adding and removing RPC clients” on page 103.</td>
</tr>
<tr>
<td>Check RPC connection every N seconds</td>
<td>Symantec Protection Engine maintains a connection with the RPC client. You can configure Symantec Protection Engine to check the RPC connection with the client periodically to ensure that the connection is active. The default value is 20 seconds. See “Configuring the RPC connection options” on page 104.</td>
</tr>
<tr>
<td>Maximum number of reconnect attempts</td>
<td>You can limit the number of times Symantec Protection Engine tries to re-establish a lost connection with the RPC client. If the client does not respond within this limit, Symantec Protection Engine stops trying to reestablish a connection. By default, Symantec Protection Engine tries to reconnect with the RPC client indefinitely. <strong>Note:</strong> Do not set a maximum number of reconnect tries if Symantec Protection Engine provides scanning for multiple RPC clients. See “Configuring the RPC connection options” on page 104.</td>
</tr>
</tbody>
</table>
Table 4-3  Protocol-specific options for RPC (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automatically send antivirus update</td>
<td>Symantec Protection Engine can automatically notify the RPC client that Symantec Protection Engine has new definitions. This notification prompts the RPC client to clear its cache of scanned files.</td>
</tr>
<tr>
<td>notifications</td>
<td>See “Notifying a file server when definitions are updated” on page 105.</td>
</tr>
</tbody>
</table>

Configuring Symantec Protection Engine to use the RPC protocol

Before you can configure any of the RPC protocol options, configure Symantec Protection Engine to use the RPC protocol.

See “Configuring Symantec Protection Engine to use the RPC protocol in the Core server only mode” on page 257.

To configure Symantec Protection Engine to use the RPC protocol

1  In the console on the primary navigation bar, click Configuration.
2  In the sidebar under Views, click Protocol.
3  In the content area under Select Communication Protocol, click RPC.
4  In the Manual Restart Required dialog box, click OK.

Whenever you switch protocols, you must restart the server. You can continue to make and apply changes in the console. However, the changes do not take effect until you restart the Symantec Protection Engine service.

5  On the toolbar, select one of the following options:

   Save  Saves your changes.
       Use this option to continue making changes in the console until you are ready to apply them.

   Apply  Applies your changes.
       Your changes are not implemented until you apply them.

See “About working with the RPC protocol” on page 100.

See “About RPC configuration options” on page 101.
Adding and removing RPC clients

You can use a single Symantec Protection Engine to support multiple RPC clients. The supported RPC clients must be located in the same domain as Symantec Protection Engine. You must provide the IP address for each RPC client for which Symantec Protection Engine provides scanning services.

See “Adding and removing RPC clients in the Core server only mode” on page 258.

To add an RPC client

1. In the console on the primary navigation bar, click **Configuration**.
2. In the sidebar under **Views**, click **Protocol**.
3. In the content area under **RPC Configuration**, in the **RPC client list** box, type an IP address for the RPC client for which Symantec Protection Engine provides scanning services.
   Type one entry per line.
4. On the toolbar, select one of the following options:
   - **Save**: Saves your changes.
     Use this option to continue making changes in the console until you are ready to apply them.
   - **Apply**: Applies your changes.
     Your changes are not implemented until you apply them.

To remove an RPC client

1. In the console on the primary navigation bar, click **Configuration**.
2. In the sidebar under **Views**, click **Protocol**.
3. In the content area under **RPC Configuration**, in the list of RPC clients, highlight the RPC clients that you want to remove from the list.
4. Press **Delete**.
5. On the toolbar, select one of the following options:
   - **Save**: Saves your changes.
     Use this option to continue making changes in the console until you are ready to apply them.
   - **Apply**: Applies your changes.
     Your changes are not implemented until you apply them.
Configuring the RPC connection options

If your client uses RPC as the communication protocol, you can specify how often you want Symantec Protection Engine to check and retry connections with the RPC client.

See “Configuring the RPC connection options in the Core server only mode” on page 259.

To configure RPC connection options

1. In the console on the primary navigation bar, click Configuration.
2. In the sidebar under Views, click Protocol.
3. In the content area under RPC Configuration, in the Check RPC connection every box, type the number of times Symantec Protection Engine should check the connection with the RPC client to ensure that the connection is active.
   The default interval is 20 seconds.
4. In the Maximum number of reconnect attempts box, type the maximum number of times that Symantec Protection Engine should try to re-establish a lost connection with the RPC client.
   The default setting is 0, which causes Symantec Protection Engine to try indefinitely to reestablish a connection. Use the default setting if Symantec Protection Engine provides scanning for multiple RPC clients.
5. On the toolbar, select one of the following options:
   - Save: Saves your changes. Use this option to continue making changes in the console until you are ready to apply them.
   - Apply: Applies your changes. Your changes are not implemented until you apply them.
Notifying a file server when definitions are updated

When the RPC client receives a request for a file from a user, it checks its cache for the file. If the file is not found, the client sends the file to Symantec Protection Engine for scanning. When Symantec Protection Engine returns a clean file to the RPC client, the client stores the file in its cache. The cached file is sent to the user and any subsequent user who requests that file. This process conserves scanning resources.

You can configure Symantec Protection Engine to automatically notify the RPC client that Symantec Protection Engine has new definitions. This notification prompts the RPC client to clear its cache of scanned files, and the process begins again. New requests for files are sent to Symantec Protection Engine for scanning and then cached. Files that are in the cache are sent to the requesting user.

**Note:** The process of sending notifications to the file server about definition updates can consume system resources, depending on how often you schedule LiveUpdate. To minimize the impact on performance, you can send the notification on demand, as needed.

You can configure Symantec Protection Engine to automatically notify the network file server of updated definitions after a LiveUpdate occurs. You can also notify the file server on demand, as needed.

See “Notifying a file server when definitions are updated in Core server only mode” on page 260.

**To automatically notify a file server when definitions are updated**

1. In the console on the primary navigation bar, click **Configuration**.
2. In the sidebar under **Views**, click **Protocol**.
3. In the content area under **RPC Configuration**, select the **Automatically send antivirus update notifications** check box.

   This option is disabled by default.
4. On the toolbar, select one of the following options:
   - **Save**: Saves your changes. Use this option to continue making changes in the console until you are ready to apply them.
   - **Apply**: Applies your changes. Your changes are not implemented until you apply them.
To notify a file server on demand when definitions are updated

1. In the console on the primary navigation bar, click **Configuration**.
2. In the sidebar under **Views**, click **Protocol**.
3. Under **Tasks**, click **Send AntiVirus Update Notification**.

See “About working with the RPC protocol” on page 100.

### Configuring the antivirus scan policy

You can configure Symantec Protection Engine to do one of the following when an infected file is found:

**To configure the antivirus scan policy**

1. On the Symantec Protection Engine administrative interface, in the left pane, click **Policies**.
2. Under **Views**, click **Scanning**.
3 Select the **Antivirus scan policy** to configure Symantec Protection Engine to do one of the following when an infected file is found:

- **Scan only**
  - Scan the file for viruses. Deny access to the infected file, but do nothing to the infected file.

- **Scan and repair files**
  - Scan the file for viruses. Try to repair the infected file, and deny access to any unrepairable file.

- **Scan and repair or delete**
  - Scan the file for viruses. Try to repair the infected file, and delete any unrepairable file from archive files.

**Note:** You must select **Scan and repair or delete** if you plan to quarantine the infected files that cannot be repaired. For more information, see the *Symantec™ Protection Engine for Network Attached Storage Implementation Guide.*

4 On the toolbar, select one of the following:

- **Save**
  - Saves your changes.
  - You can continue to make changes in the administrative interface until you are ready to apply them.

- **Apply**
  - Applies your changes.
  - Your changes are not implemented until you apply them. You must perform a manual restart for the changes to take place.

See “Configuring the antivirus scan policy in the Core server only mode” on page 261.

### Logging to the RPC client logging subsystem

Certain Symantec Protection Engine events are logged to the logging subsystem of the RPC client.

The following events are automatically logged:

- Unrepairable infections
- Container violations
Scans that are canceled because the antivirus scanning license is expired
See “About working with the RPC protocol” on page 100.

User identification and notification when a risk is found
When Symantec Protection Engine finds a risk in a file (as per configured policy) that an RPC network-attached-storage client requests, Symantec Protection Engine obtains identification information about the user who requested the infected file. The identification information includes the security identifier of the user and the IP address and host name of the requesting computer. This information is included in all related log messages that are sent to all active logging destinations for Symantec Protection Engine. This feature provides administrators with as much information as possible when a risk is found.

Note: Symantec Protection Engine can obtain only the information that the RPC client makes available. If the identification information is available, Symantec Protection Engine records it in the related log entries. Any identification information that cannot be obtained from the RPC client is omitted from the log messages and from the user notification window.

The notification message includes the following information:

■ Date and time of the event
■ Name of the infected file
■ Threat or security risk name and ID
■ Manner in which the infected file was handled (for example, the file was deleted)

See “Notifying RPC-client users that a threat was found” on page 138.

To use the user notification feature, the Windows Messenger service must be on the same computer as Symantec Protection Engine and on the user's computer.

See “Editing the service startup properties” on page 108.

Editing the service startup properties
If Symantec Protection Engine is installed on Windows and you change the protocol setting to RPC through the console, you might need to change the service startup properties to identify an account that has the appropriate permissions. You might also need to change the service startup properties if you edit the list of RPC clients.

If your client uses RPC, the account that you assign to the Symantec Protection Engine service must have all of the following rights and permissions:
Access rights to the RPC clients

Domain administrators or backup operators privileges

Local administrator permissions on the computer on which Symantec Protection Engine runs

Rights to run as a service

To edit the service startup properties

1. In the Windows Control Panel, click Administrative Tools.
2. Click Services.
3. In the list of services, right-click Symantec Protection Engine, and then click Properties.
4. In the Properties dialog box, on the Log On tab, click This account.
5. Type the account name and password for the account on which Symantec Protection Engine runs.
   Use the following format for the account name:
   domain\username
6. Click OK.
7. Stop and restart the Symantec Protection Engine service.

See “Verifying, stopping, and restarting the Symantec Protection Engine service on Windows” on page 62.
Protecting against risks

This chapter includes the following topics:

- About scanning for risks
- Enabling threat detection in Symantec Protection Engine
- About quarantining files in Symantec Protection Engine
- About preventing potential threats in Symantec Protection Engine
- About MS Office files in Symantec Protection Engine
- About container files in Symantec Protection Engine
- Customizing notifications in Symantec Protection Engine
- About Symantec Insight™
- About advanced machine learning

About scanning for risks

Symantec Protection Engine can scan all major file types (for example, Microsoft Word and Microsoft Excel files). Symantec Protection Engine can detect mobile code, such as Java, ActiveX, and stand-alone script-based threats. Symantec Protection Engine also includes a decomposer that handles most types of compressed and archive file formats and nested levels of files.

Symantec Protection Engine can detect the following types of risks:

- Viral threats (such as viruses, worms, and Trojan horses)
  See “Enabling threat detection in Symantec Protection Engine” on page 114.
- Nonviral threats (security risks such as adware and spyware)
See “Enabling nonviral threat detection in Symantec Protection Engine” on page 117.

- Denial-of-service attacks
  See “Setting container file limits” on page 161.

Symantec Protection Engine also helps you protect your network by blocking potential threats. When you receive information about a new threat, you can block or delete the message, file, or file attachment before definitions are available.

See “About preventing potential threats in Symantec Protection Engine” on page 121.

Scanning for risks can consume bandwidth, increase overall scanning time, and degrade performance. You can improve scanning performance by limiting the files and email messages to be scanned to only those that are most likely to contain risks.

See “About container files in Symantec Protection Engine” on page 130.
See “Specifying which files to scan” on page 157.
See “Specifying the maximum file or message size to scan” on page 160.

For more information about viral threats, security risks, and other forms of malicious attacks, on the Internet, go to the following URL for Symantec Security Response:

http://securityresponse.symantec.com

About threat categorization and risk ratings

Symantec Protection Engine categorizes each viral and nonviral threat under a top-level category (denoted as UberCategory). Each UberCategory has sub-categories associated with it, which are dynamic in nature and may change with definition updates. A threat can have only one sub-category assigned to it. In addition, Symantec Protection Engine also provides sub-category ID and a short description about the sub-category.

Symantec measures each viral and nonviral threat using risk rating factors along with their impact levels. The risk rating factors and their impact levels defines the degree to which a threat can harm the computer.

Table 5-1 displays the various risk rating factors and their impact levels.

<table>
<thead>
<tr>
<th>Factor</th>
<th>Description</th>
<th>Impact levels</th>
</tr>
</thead>
<tbody>
<tr>
<td>Performance impact</td>
<td>Degree to which any program can affect a system's stability, speed, and performance.</td>
<td>High, Medium, Low</td>
</tr>
</tbody>
</table>
Symantec Protection Engine calculates the overall impact (Cumulative Risk Rating) of a detected threat based on the impact levels of individual risk rating factors.

The detailed information for each detected threat is logged to all configured logging destinations and as part of the ICAP response. You can hide sub-category information and description in ICAP response by setting the EnableThreatCategoryInformation, EnableSubCategoryDescriptionResp, and EnableNonViralThreatCategoryResp parameters in the configuration.xml file.

See “Enable nonviral threat categories information” on page 380.
See “Enable subcategories description” on page 386.
See “Enable threat categories information” on page 387.

How Symantec Protection Engine detects risks

Symantec Protection Engine uses the following tools to detect risks:

Definitions  Symantec engineers track reported outbreaks of risks (such as viruses, Trojan horses, worms, adware, and spyware) to identify new risks. After a risk is identified, information about the risk (a signature) is stored in a definition file. This file contains information to detect and eliminate the risk. When Symantec Protection Engine scans for risks, it searches for these signatures.
Heuristics  Symantec Protection Engine uses Symantec Bloodhound™ heuristics technology to scan for threats for which no known definitions exist. Bloodhound heuristics technology scans for unusual behaviors (such as self-replication) to target potentially infected documents. Bloodhound technology is capable of detecting as much as 80 percent of new and unknown executable file threats. Bloodhound-Macro technology detects and repairs over 90 percent of new and unknown macro viruses. Bloodhound requires minimal overhead since it examines only programs and the documents that meet stringent prerequisites. In most cases, Bloodhound can determine in microseconds whether a file or document is likely to be infected. If it determines that a file is not likely to be infected, it moves to the next file.

Container file decomposer  Symantec Protection Engine contains a decomposer that extracts container files so that they can be scanned for risks. The decomposer continues to extract container files until it reaches the base file. Symantec Protection Engine imposes limits on file extraction. These limits protect against denial-of-service attacks that are associated with the overly large files or the complex container files that take a long time to decompose. These limits also improve scanning performance.

Symantec Protection Engine scans a file and its contents until it reaches the maximum depth that you specify. Symantec Protection Engine stops scanning any file that meets the maximum file size limit or that exceeds the maximum amount of time to decompose. It then generates a log entry. Symantec Protection Engine resumes scanning any remaining files. This process continues until Symantec Protection Engine scans all of the files to the maximum depth (that do not meet any of the processing limits).

Symantec Insight™  Symantec Insight™ is a file-based detection technology that classifies files as good or bad by examining properties, usage patterns, or users of a given file rather than scanning it.

Android Application (APK) Reputation  Symantec Protection Engine has introduced a new Android Application Reputation feature that you can use to classify the untrusted APK files. APK Reputation uses Symantec’s mobile intelligence framework that leverages data from the sources such as Norton community watch, market crawling, and malware industry partners. The files will have security ratings such as low bad, high bad, neutral, medium bad, low good, medium good, and high good.

See “About scanning for risks” on page 110.

See “About threat categorization and risk ratings” on page 111.

See “About Symantec Insight™” on page 139.
Enabling threat detection in Symantec Protection Engine

Symantec Protection Engine can detect viral and nonviral threats, such as viruses, Trojan horses, worms, and security risks in all major file types. For example, Windows, DOS, Microsoft Word, and Microsoft Excel files. To detect threats, you must enable the threat detection capability in the Symantec Protection Engine console.

Symantec Protection Engine uses Bloodhound heuristic technology to detect new and unknown threats. You can customize Bloodhound Detection from zero protection to a high level of protection. However, a high level of protection increases protection of your network but it decreases the server performance. At low levels of protection, server performance is unaffected but an unknown threat might escape detection. In most cases, the default setting (medium) is appropriate. Symantec Protection Engine also gives you an option to quarantine threats. You can quarantine threats if you have configured quarantine server in Symantec Protection Engine.

You must have a valid antivirus scanning license to scan for threats and a valid content license to update virus definitions. If you upgrade from a previous version and your licenses are current, Symantec Protection Engine automatically recognizes these licenses.

See “Enabling threat detection in the Core server only mode” on page 262.

See “How Symantec Protection Engine detects risks” on page 112.

See “Ways to test threat detection capabilities” on page 116.

To enable threat detection in Symantec Protection Engine

1. In the console on the primary navigation bar, click Policies.
2. In the sidebar under Views, click Scanning.
3. In the content area under Antivirus Scanning, select the Enable virus scanning check box.
4 In the **Bloodhound detection** level drop-down list, select the appropriate Bloodhound Detection level as follows:

<table>
<thead>
<tr>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Off</td>
<td>Disables the heuristic based file scanning.</td>
</tr>
<tr>
<td>Low</td>
<td>Optimizes the server performance, but might not detect potential threats.</td>
</tr>
</tbody>
</table>
| Medium| Provides a balance between threat detection and server performance.  
       By default, medium level is selected in Symantec Protection Engine. |
| High  | Increases the detection of threats, but might affect the server performance. |

**Note:** Turning off Bloodhound or lowering the Bloodhound level may impact the virus scanning functionality.

5 In the **Scan policy** list, select how you want Symantec Protection Engine to handle infected files. The options are as follows:
Scan policy

- **Scan only**
  Denies the access to the infected file but does nothing to the infected file.

- **Scan and delete**
  Deletes all infected files without trying to repair them, including the files that are embedded in archive files.

- **Scan and repair files**
  Tries to repair infected files but does nothing to the files that cannot be repaired. Security risks cannot be repaired.

- **Scan and repair or delete**
  Tries to repair infected files and deletes any unrepairable files from archive files. Security risks cannot be repaired.
  This is the default setting.

6 On the toolbar, select one of the following options:

**Save**
Saves your changes.
Use this option to continue making changes in the console until you are ready to apply them.

**Apply**
Applies your changes.
Your changes are not implemented until you apply them.

See “About quarantining files in Symantec Protection Engine” on page 119.
See “Configuring the quarantine in Symantec Protection Engine” on page 120.

Ways to test threat detection capabilities

You can test the threat detection capabilities of Symantec Protection Engine by using an EICAR test file.

The EICAR test file contains a test string that most major antivirus products detect and handle as though it was a threat. The test string is not a virus. You can download an EICAR test file. On the Internet, go to the following URL:

http://eicar.org
Warning: Carefully read the disclaimers on the site before you download the test file into your environment. Any tries to test antivirus software with real or dummy viruses should be handled with extreme care.

If your computer already has antivirus software, you must disable the Auto-Protect mode of the antivirus software before you download the test file.

See “Enabling threat detection in Symantec Protection Engine” on page 114.

Enabling nonviral threat detection in Symantec Protection Engine

If your client uses the ICAP protocol or the RPC protocol, you can enable the detection of one or more types of nonviral threats.

Nonviral threats are the programs that do any of the following actions:

■ Provide unauthorized access to computer systems
■ Compromise data integrity, privacy, confidentiality, or security
■ Present some type of disruption or nuisance

These programs can put your employees and your organization at risk for identity theft or fraud if they can do any of the following actions:

■ Log keystrokes
■ Capture email and instant messaging traffic
■ Harvest personal information, such as passwords and logon identifications

Nonviral threats can be introduced into your system unknowingly when users do any of the following tasks:

■ Visit a Web site
■ Download shareware or freeware software programs
■ Click links or attachments in email messages
■ Use instant messaging clients
■ Agree to an end-user license agreement from another software program

Symantec Protection Engine scans for nonviral threats in all types of content, such as email messages and Web content. Symantec Protection Engine can also scan POST transactions for nonviral threats. Symantec Protection Engine can only perform nonviral threat scanning when you enable virus scanning.

See “Enabling threat detection in Symantec Protection Engine” on page 114.

If a nonviral threat is detected, Symantec Protection Engine applies the scan policy that you configured. Symantec Protection Engine also gives you an option to
quarantine nonviral threats also. You can quarantine threats if you have configured quarantine server in Symantec Protection Engine.

See “Enabling nonviral threat detection in the Core server only mode” on page 265.

See “Configuring ICAP options” on page 98.

See “About licensing” on page 88.

To enable nonviral threat detection

1. In the console on the primary navigation bar, click **Policies**.

2. In the sidebar under **Views**, click **Scanning**.

3. In the content area under **Nonviral Threat Scanning**, select the **Security Risks** check box.

   Nonviral threat detection is only available if virus scanning is enabled.

4. On the toolbar, select one of the following options:

   - **Save** Saves your changes.
     
     Use this option to continue making changes in the console until you are ready to apply them.

   - **Apply** Applies your changes.
     
     Your changes are not implemented until you apply them.

---

Enabling advanced heuristic scanning in Symantec Protection Engine

Advanced Heuristics applies a detection method that is more aggressive than the standard detection and hence leads to better protection. On enabling this feature, there may be a slight decrease in performance and a slight increase in false positives. It is recommended to enable this feature when there is a suspected infection outbreak in the network. You can disable this feature after the outbreak has been resolved and is under control.

See “Enabling advanced heuristic scanning in the Core server only mode” on page 266.

To enable advanced heuristic scanning in Symantec Protection Engine

1. In the console on the primary navigation bar, click **Policies**.

2. In the sidebar under **Views**, click **Scanning**.

3. In the content area under **Advanced Heuristics**, check **Enable advanced heuristic scanning**.
Click OK on the Advanced Heuristics message pop-up box.

On the toolbar, select one of the following options:

- **Save**: Saves your changes. Use this option to continue making changes in the console until you are ready to apply them.
- **Apply**: Applies your changes. Your changes are not implemented until you apply them.

See “Enabling nonviral threat detection in Symantec Protection Engine” on page 117.

### About quarantining files in Symantec Protection Engine

When you use the ICAP protocol or the RPC protocol, you can quarantine the files that might contain threats. To quarantine files, you must install Symantec Central Quarantine.

See “Enabling nonviral threat detection in Symantec Protection Engine” on page 117.


For more information, see the *Symantec Central Quarantine Implementation Guide*.

You can designate unscannable files and the files that might contain threats or malicious code in Symantec Protection Engine for quarantining. Symantec Protection Engine forwards the files that you want to quarantine to Symantec Central Quarantine. Typically, the heuristically detected threats that cannot be eliminated are forwarded to the Quarantine so that they are isolated. Since the threats are isolated, they cannot spread. You can submit the files that are in the quarantine to Symantec Security Response for analysis. If a new threat is identified, new definitions are posted.

You must select **Scan and repair or delete** as the antivirus action policy to forward files to the quarantine. When a copy of a file is forwarded to the Symantec Central Quarantine, if the original, file can be repaired, it is repaired. If it cannot be repaired, it is deleted.

See “About unscannable files in Symantec Protection Engine” on page 132.

See “Configuring the quarantine server in the Core server only mode” on page 269.
Configuring the quarantine in Symantec Protection Engine

If you plan to quarantine the files that might contain threats or malicious code, configure Symantec Protection Engine to quarantine files. Also provide the host name or IP address for the computer on which Symantec Central Quarantine Server is installed.

See “Configuring the quarantine server in the Core server only mode” on page 269.

To configure the quarantine in Symantec Protection Engine

1. In the console on the primary navigation bar, click Policies.
2. In the sidebar under Views, click Quarantine.
3. In the content area under Quarantine, check Configure quarantine server.
4. In the Central quarantine server host or IP box, type the host name or the IP address for the computer on which Symantec Central Quarantine Server is installed.
5. In the Port box, type the TCP/IP port number that Symantec Protection Engine uses to pass files to Symantec Central Quarantine.
6. Select Quarantine Threats to quarantine the infected files.
   This option is available only if quarantine server is configured in Symantec Protection Engine.
7. Select Quarantine malformed files to quarantine the malformed files.
   This option is available only if quarantine server is configured in Symantec Protection Engine.
8. Select Quarantine encrypted files to quarantine encrypted container files.
   This option is available only if quarantine server is configured in Symantec Protection Engine.
9. On the toolbar, select one of the following options:

   Save       Saves your changes.
               Use this option to continue making changes in the console until you are ready to apply them.

   Apply      Applies your changes.
               Your changes are not implemented until you apply them.

See “About quarantining files in Symantec Protection Engine” on page 119.

See “Enabling threat detection in Symantec Protection Engine” on page 114.
See “Configuring Symantec Protection Engine to handle malformed container files” on page 132.
See “Configuring Symantec Protection Engine to handle encrypted container files” on page 134.

About preventing potential threats in Symantec Protection Engine

Symantec Protection Engine has features you can use to prevent emerging threats by doing the following:

Handle container files
Use this feature to handle certain types of container files, such as partial container files, that might contain threats or malicious code.
See “About container files in Symantec Protection Engine” on page 130.

Block or delete files by file name
Use this feature to filter documents by file name.
See “Configuring file name filtering in Symantec Protection Engine” on page 122.

Block or delete files by file or attachment size
Use this feature to block or delete files by file or attachment size.
See “Configuring file size filtering in Symantec Protection Engine” on page 124.

Block or delete email messages by subject line content
Use this feature to filter email messages based on subject line content.
You can also use subject line content filtering to create a comprehensive mail filtering policy. You can search the subject lines for offensive language, confidential information, and content with potential legal consequences.
Mail policies are applied only to MIME-encoded messages and do not affect non-MIME-encoded file types.
See “Configuring subject line content filtering in Symantec Protection Engine” on page 126.
Block or delete email messages by message origin

Use this feature to filter email messages based on message origin. You can block or delete email messages from a specific domain or email address. You can also use message origin filtering to create a comprehensive mail filtering policy.

Mail policies are applied only to MIME-encoded messages and do not affect non-MIME-encoded file types.

See “Configuring message origin filtering in Symantec Protection Engine” on page 128.

Configuring file name filtering in Symantec Protection Engine

If your client uses the ICAP protocol, you can filter files by file name to protect your network during an outbreak. For example, if you know the file name of a new email-borne threat, you can use this information to block infected email messages.

You can configure Symantec Protection Engine to handle the file in one of the following ways:

**Block access to the file or the message**
Blocks access to any top-level file that matches the file name.

If a container file or email message contains a file or attachment that matches the file name, access to the entire container or message is blocked.

**Delete the file or the attachment**
Deletes any file that matches the file name and logs the violation.

Symantec Protection Engine deletes any attachments within an email message that match the file name. Attachments that do not match the file name are not deleted and are delivered with the message. If you activate the mail message update feature, the message indicates that an attachment has been deleted due to a policy violation.

Symantec Protection Engine deletes any embedded files that match the specified file name within a container file that contains multiple files. The embedded files that do not match the specified file name are not deleted. Deleted files are replaced with a replacement file, DELETEN.TXT, which indicates the reason that the file was deleted.

See “Customizing notifications in Symantec Protection Engine” on page 135.

Use wildcard characters if you are unsure of an exact file name or to block all file attachments with a specific extension. For example, you can use the wildcard *virus* to block all attachments with the word virus in the file name.
Note: If your client uses the antivirus-only application programming interface (API), file name violations are reported to the client in the server's response as mail-policy violations. If you use the extended API or have a standard ICAP implementation, this type of violation is reported as a file violation.

See “Configuring file name filtering in the Core server only mode” on page 270.

To configure file name filtering in Symantec Protection Engine

1 In the console on the primary navigation bar, click Policies.

2 In the sidebar under Views, click Filtering.

3 In the content area on the Files tab, under Blocking by File Name, check Block files with the following names.

4 Under When a matching file is found, select one of the following to specify how Symantec Protection Engine handles the messages that contain an attachment with that file name:
   - Block access to the file or message
     This option is enabled by default.
   - Delete the file or attachment

5 In the file name box, do any of the following:
   - Add a file name to the list. Type the file name that you want to add. Type one entry per line. Search strings are not case-sensitive.
     You can use the following wildcard characters as needed:
     - A question mark (?) to represent a single character.
     - An asterisk (*) to represent zero or more characters.
     - A backslash (\) as an escape character. For example, precede a ? or a * with \ to match a literal ? or * symbol in a file name. To match a literal \ symbol, use \\.
Remove a file name from the list. Highlight the file name that you want to remove, and press Delete.

6 On the toolbar, select one of the following options:

Save
Saves your changes.
Use this option to continue making changes in the console until you are ready to apply them.

Apply
Applies your changes.
Your changes are not implemented until you apply them.

See “About preventing potential threats in Symantec Protection Engine” on page 121.
See “Configuring file size filtering in Symantec Protection Engine” on page 124.
See “Configuring subject line content filtering in Symantec Protection Engine” on page 126.
See “Configuring message origin filtering in Symantec Protection Engine” on page 128.

Configuring true type file filtering in Symantec Protection Engine

You can configure Symantec Protection Engine to handle the file based on its type. It blocks access to any top-level file that matches the file type. If a container file or email message contains a file or attachment that matches the file type, access to the entire container or message is blocked.

You can use wildcard characters for the files based on their categories to block the files. For example, you can use the wildcard image/* to block all files that fall under the image category.

Note: Configuration of the file true type filtering is supported only on ICAP protocol.

See “Configuring true type file filtering in the Core server only mode” on page 275.

Configuring file size filtering in Symantec Protection Engine

If your client uses the ICAP protocol, you can filter files based on their sizes. For example, suppose you know the exact size of new email-borne threat. You can use this information to block any email messages that match this size.
You can configure Symantec Protection Engine to handle the file in one of the following ways:

- **Block access to the file or the message**: Blocks access to any top-level file that matches the file size. If a container file or email message contains a file or attachment that matches the specified file size, Symantec Protection Engine blocks the entire container or message.

- **Delete the file or attachment**: Deletes any files that match the specified file size and logs the violation. Symantec Protection Engine deletes any attachments within an email message that match a specified file size. Attachments that do not match the specified file size are delivered with the message. If you activate the mail message update feature, the mail message indicates that an attachment has been deleted due to a file policy violation.

  Symantec Protection Engine deletes any embedded files within a container file that contains multiple files that match the specified file size. The embedded files that do not match the specified file size are not deleted. Deleted files are replaced with a replacement file, DELETEN.TXT, which indicates the reason that the file was deleted.

  See “Customizing notifications in Symantec Protection Engine” on page 135.

**Note**: If your client uses the antivirus-only application programming interface (API), file size violations are reported to the client in the server's response as mail-policy violations. If you use the extended API or have a standard ICAP implementation, this type of violation is reported as a file violation.

See “Configuring file size filtering in the Core server only mode” on page 273.

### To configure file size filtering in Symantec Protection Engine

1. In the console on the primary navigation bar, click **Policies**.
2. In the sidebar under **Views**, click **Filtering**.
3. In the content area on the **Files** tab, under **Blocking by File Size**, check **Block files with the following sizes**.
4. Under **When a matching file is found**, select one of the following options to specify how you want Symantec Protection Engine to handle the messages that contain an attachment with that file size:
   - Block access to the file or the message
     - This option is enabled by default.
   - Delete the file or attachment
5 In the **file size** box, do any of the following:

- **Add a file size (in bytes) to the list.** Type the file size that you want to add. Type one entry per line.
- **Highlight the file size that you want to remove, and press Delete.**

6 On the toolbar, select one of the following options:

- **Save** Saves your changes.
  - Use this option to continue making changes in the console until you are ready to apply them.
- **Apply** Applies your changes.
  - Your changes are not implemented until you apply them.

See “About preventing potential threats in Symantec Protection Engine” on page 121.

See “Configuring file name filtering in Symantec Protection Engine” on page 122.

See “Configuring subject line content filtering in Symantec Protection Engine” on page 126.

See “Configuring message origin filtering in Symantec Protection Engine” on page 128.

**Configuring subject line content filtering in Symantec Protection Engine**

If your client uses the ICAP protocol, you can configure Symantec Protection Engine to block messages by the subject line. You can use this feature to handle new-borne threats for which a threat definition has not been created. You can also use this feature to filter mail messages for inappropriate or confidential information or potential spam.

Symantec Protection Engine scans the subject lines of incoming mail messages for the text string that you specify. You can use wildcard characters when you are not sure of the exact subject line. Symantec Protection Engine ignores any white space (tabs or spaces) at the beginning of the subject line. It also ignores any white space that you enter at the beginning of your text string.

**Note:** Symantec Protection Engine automatically encodes and saves the text strings in Unicode/UTF-8 when you apply your changes in the console.
See “Configuring subject line content filtering in the Core server only mode” on page 276.

To configure subject line content filtering in Symantec Protection Engine

1. In the console on the primary navigation bar, click **Policies**.
2. In the sidebar under **Views**, click **Filtering**.
3. In the content area on the **Mail** tab, under **Blocking by Subject Line**, check **Use the following subjects**.
4. In the **subject line text** box, do any of the following:

   - **Add a subject line to the list.**
     - Type the subject line or text string in the subject line that you want to block. Type as many subject lines to block as needed. Type one entry per line. Search strings are not case-sensitive. You can use the following wildcard characters as needed:
     - A question mark (?) to represent a single character.
     - An asterisk (*) to represent zero or more characters.
     - A backslash (\) as an escape character. For example, precede a ? or a * symbol with \ to match a literal ? or * symbol in a file name. To match a literal symbol \, use \\\n   - **Remove a subject line from the list.**
     - Highlight the subject line entry that you want to remove, and press **Delete**.

5. Check **Block messages with empty subject lines** to block the mail messages that have blank subject lines.

6. On the toolbar, select one of the following options:

   - **Save**
     - Saves your changes.
     - Use this option to continue making changes in the console until you are ready to apply them.
   - **Apply**
     - Applies your changes.
     - Your changes are not implemented until you apply them.

See “About preventing potential threats in Symantec Protection Engine” on page 121.
See “Configuring file name filtering in Symantec Protection Engine” on page 122.
See “Configuring file size filtering in Symantec Protection Engine” on page 124.
See “Configuring message origin filtering in Symantec Protection Engine” on page 128.
Configuring message origin filtering in Symantec Protection Engine

If your client uses the ICAP protocol, you can configure Symantec Protection Engine to block mail messages from a specific domain or email address. The domain name search string that you enter is matched against the addresses in the From header of the email message. If the search string matches an address, the message is rejected.

The following table contains examples of the ways that you can define the email addresses and domains that you want to block:

<table>
<thead>
<tr>
<th>Email Address</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="mailto:name@example.symantecdomain.com">name@example.symantecdomain.com</a></td>
<td>Blocks mail from a single email address. You can use the wildcard characters $ and * in the user portion of the name. The $ wildcard character matches a single character. The * wildcard character matches zero or more characters. You cannot use both wildcard characters in the same entry. For example, *example$@internet.domain is not supported. You cannot use wildcard characters in subdomain or domain addresses. The subdomain and domain must match exactly.</td>
</tr>
<tr>
<td>@example.symantecdomain.com</td>
<td>Blocks all mail from a specific domain and subdomain address. For example, mail from <a href="mailto:name@example.symantecdomain.com">name@example.symantecdomain.com</a> is allowed. You must precede the address with an @ symbol to ensure that only mail from that specific address is blocked. The use of wildcard characters in subdomain or domain addresses is not supported.</td>
</tr>
<tr>
<td>.symantecdomain.com</td>
<td>Blocks all mail from an entire domain, including any subdomains. For example, mail from example.symantecdomain.com or internet.symantecdomain.com would be blocked. You must precede the domain address with a period to ensure that any subdomains are blocked. You cannot use wildcard characters in subdomain or domain addresses.</td>
</tr>
</tbody>
</table>

See “Configuring message origin filtering in the Core server only mode” on page 278.

To configure message origin filtering in Symantec Protection Engine

1. In the console on the primary navigation bar, click Policies.
2. In the sidebar under Views, click Filtering.
3. In the content area on the Mail tab, under Blocked Senders, check Use the following domains.

4. In the blacklist text box, do any of the following tasks:

   - Add a domain address or email address to the list. Type a domain address or email address. Type one per line. You can enter up to 5000 addresses. Search strings are not case-sensitive.

   - Remove a domain address or email address from the list. Highlight the address that you want to remove, and press Delete.

5. On the toolbar, select one of the following options:

   - Save Saves your changes. Use this option to continue making changes in the console until you are ready to apply them.

   - Apply Applies your changes. Your changes are not implemented until you apply them.

See “About preventing potential threats in Symantec Protection Engine” on page 121.
See “Configuring file name filtering in Symantec Protection Engine” on page 122.
See “Configuring file size filtering in Symantec Protection Engine” on page 124.
See “Configuring subject line content filtering in Symantec Protection Engine” on page 126.

About MS Office files in Symantec Protection Engine

Previously, Symantec Protection Engine was not able to repair the threats that were embedded in MS Office files and used to block access to such files. From version 7.0 onwards, Symantec Protection Engine’s scanning capabilities have been enhanced for such office files. Symantec Protection Engine is now capable of scanning the file and can also repair or delete the embedded content. Thus, you would now be able to retrieve the clean contents from the file.

Symantec Protection Engine supports the following formats:

- OLE inside OLE
  Objecting Linking and Embedding (OLE) formats like doc, x1s, and dot
About container files in Symantec Protection Engine

You can handle container files based on certain criteria that might indicate the presence of a threat or malicious code and prevent Symantec Protection Engine from effectively scanning the file.

Table 5-2 describes the types of container files that you can handle in Symantec Protection Engine.

Table 5-2  Types of container files

<table>
<thead>
<tr>
<th>Type of file</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Partial MIME container files</td>
<td>Symantec Protection Engine must receive a MIME-encoded message in its entirety to scan it for threats. Some email software applications break down large messages into a number of smaller, more manageable messages for transmission. These messages are typically transmitted separately and reassembled before delivery to the recipient. Because the message is broken down into several partial messages, the entire message (including all attachments) is not available to Symantec Protection Engine for scanning. Symantec Protection Engine is configured by default to reject partial messages because they cannot effectively be scanned for threats. See “Configuring Symantec Protection Engine to handle partial container files” on page 131.</td>
</tr>
<tr>
<td>Malformed container files</td>
<td>Computer viruses and malicious programs sometimes create intentionally malformed files. Symantec Protection Engine recognizes such files. If Symantec Protection Engine can identify the container type, in some cases, it can repair the container file. If Symantec Protection Engine cannot determine the container type, Symantec Protection Engine rejects it as a potentially infected file. See “Configuring Symantec Protection Engine to handle malformed container files” on page 132.</td>
</tr>
</tbody>
</table>
Table 5-2  Types of container files (continued)

<table>
<thead>
<tr>
<th>Type of file</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encrypted container files</td>
<td>Infected files are often encrypted to defeat scanning attempts. Encrypted files cannot be</td>
</tr>
<tr>
<td></td>
<td>decrypted and scanned without the appropriate decryption tool. You can configure Symantec</td>
</tr>
<tr>
<td></td>
<td>Protection Engine to handle encrypted container files to protect your network from threats.</td>
</tr>
<tr>
<td></td>
<td>See “Configuring Symantec Protection Engine to handle encrypted container files” on page 134.</td>
</tr>
</tbody>
</table>

See “About unscannable files in Symantec Protection Engine” on page 132.

**Configuring Symantec Protection Engine to handle partial container files**

Some email software applications break down large messages into a number of smaller, more manageable messages for transmission. These messages are typically transmitted separately and reassembled before delivery to the recipient. Symantec Protection Engine is unable to scan partial messages. You can configure Symantec Protection Engine to handle partial container files.

See “Configuring Symantec Protection Engine to handle partial container files in the Core server only mode” on page 279.

To configure Symantec Protection Engine to handle partial container files

1. In the console on the primary navigation bar, click **Policies**.
2. In the sidebar under **Views**, click **Filtering**.
3. In the content area on the **Container Handling** tab, under **Partial Container Handling**, check **Deny partial MIME**.
   
   By default, Symantec Protection Engine denies access to partial MIME container files.
4. On the toolbar, select one of the following options:

   **Save** Saves your changes.
   
   Use this option to continue making changes in the console until you are ready to apply them.

   **Apply** Applies your changes.
   
   Your changes are not implemented until you apply them.
About unscannable files in Symantec Protection Engine

Symantec Protection Engine cannot scan certain file types as they cannot be extracted or they do not match standard file formats. From version 7.0 onwards, such files (encrypted and malformed containers), would be referred to as "Unscannable" files.

Previously, Symantec Scan Engine had limited policies to handle such unscannable files. Now, Symantec Protection Engine provides better control over handling unscannable files.

Symantec Protection Engine provides the following options to handle unscannable files:

- Log only
  Generates a log entry.

- Block
  Blocks the unscannable files and generates a log entry.

- Delete
  Deletes the unscannable files and generates a log entry.

In addition, you can also choose to quarantine unscannable files with any of the above options.

See “Configuring Symantec Protection Engine to handle malformed container files” on page 132.

See “Configuring Symantec Protection Engine to handle encrypted container files” on page 134.

Configuring Symantec Protection Engine to handle malformed container files

Malformed container files are unscannable in Symantec Protection Engine. If you want to protect your network from threats of malformed container files, configure Symantec Protection Engine to handle unscannable malformed container files.

See “Configuring Symantec Protection Engine to handle malformed container files in the Core server only mode” on page 280.
To configure Symantec Protection Engine to handle malformed container files

1. In the console on the primary navigation bar, click **Policies**.

2. In the sidebar under **Views**, click **Filtering**.

3. In the content area on the **Container Handling** tab, under **Malformed Container Handling**, select the **Enable Malformed Container Handling** check box.

4. Under **Enable Malformed Container Handling**, select one of the following to specify how Symantec Protection Engine should handle malformed files:

   - **Log only**: Generates a log entry.
   - **Block**: Blocks the malformed container files and generates a log entry. By default, Symantec Protection Engine blocks malformed container files.
   - **Delete**: Deletes the malformed container files and generates a log entry.

   The options are available only if the **Enable Malformed Container Handling** is enabled.

5. On the toolbar, select one of the following options:

   - **Save**: Saves your changes. Use this option to continue making changes in the console until you are ready to apply them.
   - **Apply**: Applies your changes. Your changes are not implemented until you apply them.

See “About container files in Symantec Protection Engine” on page 130.

See “Configuring Symantec Protection Engine to handle partial container files” on page 131.

See “Configuring Symantec Protection Engine to handle encrypted container files” on page 134.

See “Configuring the quarantine in Symantec Protection Engine” on page 120.
Configuring Symantec Protection Engine to handle encrypted container files

Encrypted files are unscannable in Symantec Protection Engine. If you want to protect your network from threats of encrypted container files, configure Symantec Protection Engine to handle unscannable encrypted container files.

See “Configuring Symantec Protection Engine to handle encrypted container files in the Core server only mode” on page 282.

To configure Symantec Protection Engine to handle encrypted container files

1. In the console on the primary navigation bar, click **Policies**.
2. In the sidebar under **Views**, click **Filtering**.
3. In the content area on the **Container Handling** tab, under **Encrypted Container Handling**, select **Enable Encrypted Container Handling** check box.
4. Under **Enable Encrypted Container Handling**, select one of the following to specify how Symantec Protection Engine handles encrypted files:
   - **Log only**: Generates a log entry.
     - By default, Symantec Protection Engine only logs instances of encrypted container files.
   - **Block**: Blocks the encrypted container files and generates a log entry.
   - **Delete**: Deletes the encrypted container files and generates a log entry.

   The options are available only if the **Enable Encrypted Container Handling** is enabled.

5. On the toolbar, select one of the following options:
   - **Save**: Saves your changes.
     - Use this option to continue making changes in the console until you are ready to apply them.
   - **Apply**: Applies your changes.
     - Your changes are not implemented until you apply them.

See “About container files in Symantec Protection Engine” on page 130.
Customizing notifications in Symantec Protection Engine

You can configure Symantec Protection Engine to customize messages to users to notify them when a file is infected, repaired, denied access to, malformed, encrypted, or deleted. You can add the text to the body of an infected MIME-encoded message or to the body of a replacement file for a deleted attachment.

Symantec Protection Engine attaches a text file to the email message in the place of each attachment that is deleted because it cannot be repaired. The text file that is inserted is called DELETEN.TXT, where N is a sequence number. For example, if two attachments are deleted, the replacement files are called DELETE0.TXT and DELETE1.TXT.

When you use ICAP, Symantec Protection Engine displays an HTML text message to the user when a requested file is blocked. Access to a file is blocked when the file contains a threat and cannot be repaired.

See “Customizing notifications in the Core server only mode” on page 284.

Table 5-3 describes the types of notification messages that you can customize.

<table>
<thead>
<tr>
<th>Type of notification</th>
<th>Default text</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deleted file</td>
<td>File: ${FILE_NAME} was infected with ${THREAT_NAME} (${THREAT_ID}). File ${QUARANTINED}. File was deleted.</td>
</tr>
<tr>
<td>Repaired file</td>
<td>File: ${FILE_NAME} was infected with ${THREAT_NAME} (${THREAT_ID}). File ${QUARANTINED}. File was repaired.</td>
</tr>
<tr>
<td>Infected file</td>
<td>File: ${FILE_NAME} was infected with ${THREAT_NAME} (${THREAT_ID}). File ${QUARANTINED}. File is still infected</td>
</tr>
<tr>
<td>Total threat found</td>
<td>This email message was infected. ${TOTAL_THREATS} number of threats were found.</td>
</tr>
</tbody>
</table>
Table 5-3  User notification messages (continued)

<table>
<thead>
<tr>
<th>Type of notification</th>
<th>Default text</th>
</tr>
</thead>
<tbody>
<tr>
<td>Denied file size</td>
<td>The file attached to this email was removed because the file size is not allowed. File attachment: ${FILE_NAME}. Matched file size: ${FILE_SIZE}.</td>
</tr>
<tr>
<td>Denied file names</td>
<td>The file attached to this email was removed because the file name is not allowed. File attachment: ${FILE_NAME}. Matched pattern: ${MATCHING_FILENAME_ENTRY}.</td>
</tr>
<tr>
<td>Encrypted file</td>
<td>The encrypted container attached to this email was removed. File attachment: ${FILE_NAME}. File ${QUARANTINED}.</td>
</tr>
<tr>
<td>Malformed file</td>
<td>The malformed container attached to this email was removed. File attachment: ${FILE_NAME}. File ${QUARANTINED}.</td>
</tr>
<tr>
<td>Web browser</td>
<td>The content you just requested contains ${THREAT_NAME} and was blocked by the Symantec Protection Engine based on local administrator settings. Contact your local administrator for further information.</td>
</tr>
<tr>
<td>APK deleted</td>
<td>File: ${FILE_NAME} violates APK reputation policy. File ${QUARANTINED}. File was deleted.</td>
</tr>
</tbody>
</table>

You can configure Symantec Protection Engine to customize Insight messages to notify users when a file is infected, replaced, or deleted. You can add the text to the body of an infected MIME-encoded message or to the body of a replacement file for a deleted attachment.

to work with the Core server only mode.

Table 5-4 describes the types of Insight notification messages that you can customize.

Table 5-4  Insight notification messages

<table>
<thead>
<tr>
<th>Type of notification</th>
<th>Default text</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deleted file</td>
<td>File: ${FILE_NAME} was infected with ${THREAT_NAME} (${THREAT_ID}). File ${QUARANTINED}. File was deleted.</td>
</tr>
<tr>
<td>Infected file</td>
<td>File: ${FILE_NAME} was infected with ${THREAT_NAME} (${THREAT_ID}). File ${QUARANTINED}. File is still infected.</td>
</tr>
</tbody>
</table>

Table 5-5 lists the variables that you can use to customize your notifications.
### Table 5-5 Notification variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>${FILE_NAME}</code></td>
<td>The name of the infected file.</td>
</tr>
<tr>
<td><code>${FILE_SIZE}</code></td>
<td>The size of the file that violates the maximum file size threshold.</td>
</tr>
<tr>
<td></td>
<td>See “Configuring file size filtering in Symantec Protection Engine” on page 124.</td>
</tr>
<tr>
<td><code>${THREAT_NAME}</code></td>
<td>The name of the threat.</td>
</tr>
<tr>
<td><code>${THREAT_ID}</code></td>
<td>The threat identification number.</td>
</tr>
<tr>
<td><code>${QUARANTINED}</code></td>
<td>Indicates whether a file was quarantined.</td>
</tr>
<tr>
<td></td>
<td>See “About quarantining files in Symantec Protection Engine” on page 119.</td>
</tr>
<tr>
<td><code>${TOTAL_THREATS}</code></td>
<td>The total number of risks that are detected in the MIME message.</td>
</tr>
<tr>
<td><code>${MATCHING_FILENAME_ENTRY}</code></td>
<td>The file name pattern that triggered the violation.</td>
</tr>
<tr>
<td></td>
<td>See “Configuring file name filtering in Symantec Protection Engine” on page 122.</td>
</tr>
</tbody>
</table>

to customize user notifications in Symantec Protection Engine

1. In the console on the primary navigation bar, click **Policies**.
2. In the sidebar under **Views**, click **Notifications**.
3. Under **User Message Notifications**, check **Add text to the body of infected MIME-encoded messages to warn recipients of infections (threats and security risks)**.
4. Check **Add text to the body of replacement file for a deleted attachment**.
5. Customize any of the user notification messages.
6. On the toolbar, select one of the following options:

   **Save** Saves your changes.
   Use this option to continue making changes in the console until you are ready to apply them.

   **Apply** Applies your changes.
   Your changes are not implemented until you apply them.
Notifying RPC-client users that a threat was found

If your client uses RPC, you can configure Symantec Protection Engine to notify a user that a file cannot be retrieved from an RPC-network-attached-storage client because it contains a threat.

The notification message includes the following information:

- Date and time of the event
- Name of the infected file
- Threat name and ID
- Manner in which the infected file was handled (for example, whether the file was repaired or deleted)

The notification message also includes information about the Symantec Protection Engine that detected the infection. For example, the message contains the IP address and the port number of Symantec Protection Engine. The message also contains the date and the revision number of the definitions that were used to detect the threat.

This feature is only available on Windows. The requesting user's computer must be in the same domain as Symantec Protection Engine. The Windows Messenger service must be running both on the computer on which Symantec Protection Engine is running and on the user's computer. If the notification information cannot be delivered to the requesting user, a failure message is logged.

See “Notifying RPC client users that a threat was found in the Core server only mode” on page 289.

To notify RPC-client users that a threat was found

1. In the console on the primary navigation bar, click **Monitors**.
2. In the sidebar under **Views**, click **Alerting**.
3. In the content area under **Log Windows Messenger**, check **Enable Windows Messaging alerting**.

   User notification is disabled by default.

4. On the toolbar, select one of the following options:

   - **Save**: Saves your changes. Use this option to continue making changes in the console until you are ready to apply them.
   - **Apply**: Applies your changes. Your changes are not implemented until you apply them.
See “About scanning for risks” on page 110.

About Symantec Insight™

Symantec Insight™ is a file-based detection technology that classifies files as good or bad by examining properties, usage patterns, or users of a given file rather than scanning it. Insight-based security puts files in context, using their age, frequency, location, and more to expose threats otherwise missed.

Note: Symantec Insight™ provides reputation information for only Portable Executable (PE) files.

How does Symantec Protection Engine use Symantec Insight™

Symantec Protection Engine integrates the Symantec Insight™ technology and adapts it to cater to its various deployment scenarios. Symantec Protection Engine is preconfigured with different Insight threshold values for the following popular deployment methods:

- Email Server
- Proxy/Web cache server
- Other Application
- NAS

The Insight Threshold value depends upon the deployment method and the Insight Aggression Level.

Note: Insight Scanning can work only if AV scanning is enabled in Symantec Protection Engine. If scanning is disabled in Symantec Protection Engine, the Insight feature is also disabled.

Symantec Protection Engine provides the following options to handle infected files that are detected by Symantec Insight™:

- Log only: Generates a log entry of the infected files that are detected by Symantec Insight. This is the default option.
- Block: Blocks the infected files that are detected by Symantec Insight and generates a log entry.
- Delete: Deletes the infected files that are detected by Symantec Insight and generates a log entry.
Symantec Protection Engine quarantines the infected files that are detected by Symantec Insight. This option is enabled only if the Quarantine server is configured.

**Note:** If Symantec Insight is disabled by using the command-line utility XMLModifier, the options on the user interface are still available but the configuration does not work.

### About Symantec Insight™ result parameters

If Symantec Insight™ detects a file as infected, the Insight result consists of the following information:

**Note:** The Insight result parameters are available in the ICAP response only if the file has been convicted by Insight and the EnableReputationInfo parameter is set to true in the configuration.xml file.

Table 5-6 describes the various parameters returned by Insight.

#### Table 5-6  Symantec Insight™ results and their possible values

<table>
<thead>
<tr>
<th>Factor</th>
<th>Description</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reputation</td>
<td>Reputation of the file</td>
<td>■ TRUSTED</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ GOOD</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ UNPROVEN</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ POOR</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ UNTRUSTED</td>
</tr>
<tr>
<td>Prevalence</td>
<td>Prevalence of the file</td>
<td>■ FEW</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ TENS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ HUNDREDS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ THOUSANDS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ MILLIONS</td>
</tr>
<tr>
<td>Age</td>
<td>Age of file</td>
<td>■ VERY_RECENT</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ DAYS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ WEEKS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ MONTHS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ YEARS</td>
</tr>
<tr>
<td>File type</td>
<td>Type of file</td>
<td>Only Portable Executable (PE) files</td>
</tr>
</tbody>
</table>
Table 5-6  Symantec Insight™ results and their possible values (continued)

<table>
<thead>
<tr>
<th>Factor</th>
<th>Description</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>SHA256</td>
<td>SHA256 hash value of a file, which uniquely identifies the file</td>
<td></td>
</tr>
</tbody>
</table>

Enabling Symantec Insight™ policy

You must have a valid Insight scanning license to scan for threats and to update Insight feeds. Insight scanning is enabled by default.

Symantec Protection Engine also gives you an option to quarantine threats. You can quarantine threats if you have configured the Quarantine server in Symantec Protection Engine.

**Note:** If Insight is enabled then all main categories (including security risks, advanced heuristics) are enabled by default in Symantec Protection Engine irrespective of whether Security Risks and Advanced heuristics scanning policy for Antivirus scanning is disabled or enabled.

See "Enabling Symantec Insight™ in the Core server only mode" on page 290.

To configure Symantec Insight™ policy

1. In the console on the primary navigation bar, click Policies.
2. In the sidebar under Views, click Insight.
3. In the content area, under Insight Policies, select one of the following options:
   - Log only: Generates a log entry for the files that are detected by Symantec Insight
   - Block: Blocks the files that are detected by Symantec Insight and generates a log entry
Delete: Deletes the files that are detected by Symantec Insight files and generates a log entry

4 On the toolbar, select one of the following options:

- **Save**: Saves your changes.
  
  Use this option to continue making changes in the console until you are ready to apply them.

- **Apply**: Applies your changes.
  
  Your changes are not implemented until you apply them.

See “About quarantining files in Symantec Protection Engine” on page 119.

### Configuring the Symantec Insight™ aggression level

The Insight Aggression Level defines how sensitive the Insight feature is to a file’s reputation score. Higher the aggression level, more are the number of files that are detected as threats. However, there is a possibility of false positives.

See “Configuring the Symantec Insight™ aggression level in the Core server only mode” on page 292.

**To configure the Insight aggression level**

1. In the console on the primary navigation bar, click **Policies**.
2. In the sidebar under **Views**, click **Insight**.
3. Under **Insight Aggression Level**, select the appropriate aggression level.
4. On the toolbar, select one of the following options:

   - **Save**: Saves your changes.
     
     Use this option to continue making changes in the console until you are ready to apply them.

   - **Apply**: Applies your changes.
     
     Your changes are not implemented until you apply them.

See “To configure Symantec Insight™ policy” on page 141.

### Excluding files from Insight scanning based on file size

You can enter a file size criteria to exclude files from scanning.
See “Excluding files from Insight scanning based on file size in the Core server only mode” on page 292.

To exclude files based on file size

1. In the console on the primary navigation bar, click Policies.
2. In the sidebar under Views, click Insight.
3. In the Avoid Insight query for files larger than field, enter the file size (in bytes), above which Insight excludes the file from scanning.
   The default value is 128 MB.
4. On the toolbar, select one of the following options:
   - Save: Saves your changes.
     Use this option to continue making changes in the console until you are ready to apply them.
   - Apply: Applies your changes.
     Your changes are not implemented until you apply them.

See “To configure Symantec Insight™ policy” on page 141.

Excluding files from Insight scanning based on SHA256

You can enter the SHA256 value of files that you want to exclude from scanning.

Note: Only 500 entries are allowed. Any entry above 500 is removed automatically.

See “Excluding files from Insight scanning based on SHA256 in the Core server only mode” on page 293.

To exclude files based on SHA256

1. In the console on the primary navigation bar, click Policies.
2. In the sidebar under Views, click Insight.
3 In the **SHA256 Exclude List** field, enter the SHA256 value (hash value of the file that uniquely identifies the file) of the files that Insight should exclude from scanning.

4 On the toolbar, select one of the following options:

- **Save**
  - Saves your changes.
  - Use this option to continue making changes in the console until you are ready to apply them.

- **Apply**
  - Applies your changes.
  - Your changes are not implemented until you apply them.

See “To configure Symantec Insight™ policy” on page 141.

### About advanced machine learning

Symantec Protection Engine is now incorporated with the advanced machine learning technology that detects malware based on static attributes. This technology enables Symantec Protection Engine to detect malware in the pre-execution phase, thereby stopping large classes of malware, both known and unknown. In Symantec Protection Engine, this technology works with the File Insight (Reputation) technology to provide best-in-class protection with low false positives.

This feature is enabled in Symantec Protection Engine by default. You can disable this feature by using XMLModifier command-line utility.

See “Enabling advanced machine learning in the Core server only mode” on page 268.
Modifying and tuning the performance of Symantec Protection Engine

This chapter includes the following topics:

- How to monitor Symantec Protection Engine performance
- Ways to improve Symantec Protection Engine performance
- About telemetry data

How to monitor Symantec Protection Engine performance

You should continually monitor Symantec Protection Engine to ensure that it operates at an optimal level for your environment. Continual monitoring ensures that you can make the necessary adjustments as soon as you detect a degradation in performance.


You can monitor Symantec Protection Engine performance in the following ways:

- Monitoring scanning requests
- Monitoring Symantec Protection Engine resources
Monitoring scanning requests

Symantec Protection Engine provides a feature that lets you define the expected scanning load for specific time periods. When the Symantec Protection Engine scanning load decreases significantly, it might indicate a performance issue. You can use this feature to detect possible problems before they become critical. If Symantec Protection Engine detects fewer scan requests than the expected load, it logs the event to the designated logging destinations and alert destinations. The event is logged at the Warning level.

See “Logging levels and events” on page 202.

Symantec Protection Engine averages the number of scan requests for one minute. If the average number of requests for that minute meets or exceeds the threshold, no alert is sent. If the average number of scan requests for that minute is below the threshold, Symantec Protection Engine sends an alert.

For example, if you set a threshold of 20 requests per second for Wednesday from 1:00 A.M. to 2:00 A.M., Symantec Protection Engine does not generate an alert for any minute in which it receives 1,200 or more requests (20 requests times 60 seconds). Symantec Protection Engine only generates an alert for any minute in which it receives fewer than 1,200 requests.

All of the schedules that you create appear in the Existing Schedules table. Active schedules are denoted in green; inactive schedules are denoted in red.

You can control how scanning requests are monitored in the following ways:

- Enable or disable the scan request monitor feature.
- Add a new schedule.
- Deactivate an existing schedule.
- Activate a deactivated schedule.
- Delete a schedule.

See “Monitoring scanning requests in the Core server only mode” on page 295.

To enable or disable the scan request monitor feature

1. In the console on the primary navigation bar, click Monitors.
2. In the sidebar under Views, click Requests.
3. In the content area under Monitor Requests, do one of the following steps:
   - To enable the feature, check Monitor requests.
     You must enable the feature to add, activate, deactivate, or delete any schedules.
   - To disable the feature, uncheck Monitor requests.
This feature is disabled by default.

4 On the toolbar, select one of the following options:

- **Save** Saves your changes.
  Use this option to continue making changes in the console until you are ready to apply them.

- **Apply** Applies your changes.
  Your changes are not implemented until you apply them.

**To add a new schedule**

1 In the content area under **Plan a Schedule**, click the **Day** drop-down list, and select the day of the week that you want to monitor.

   You can only select one day.

2 Click the **From** drop-down list, and select the beginning hour for the schedule time range.

   This setting uses a 24-hour clock. For example, 14 is 2:00 PM. You can select a range from 0 (12:00 AM of the day selected by the user) to 23 (11:00 PM). Hours that you have already used to create schedules for that day do not appear in the list.

3 Click the **To** drop-down list, and select the ending hour for the schedule time range.

   This option uses a 24-hour clock. For example, 14 is 2:00 PM. You can select a range from 0 (12:00 AM of the previous day) to 23 (11:00 PM). For example, if you select Tuesday, select 23 from the From drop-down list, and then select 0 from the To drop-down list, you are monitoring the threshold for the last hour of the day on Tuesday.

   Hours that you have already used to create schedules for that day do not appear in the list.

4 In the **Threshold** box, type the threshold that represents the expected file load at which you want Symantec Protection Engine to issue an alert.

   Specify a threshold that would signify a possible issue but not generate a high number of false alarms.
5 In the sidebar under Tasks, click Add Schedule.

The schedule appears in the Existing Schedules table. New schedules are activated by default.

6 On the toolbar, select one of the following options:

- **Save** Saves your changes.
  
  Use this option to continue making changes in the console until you are ready to apply them.

- **Apply** Applies your changes.
  
  Your changes are not implemented until you apply them.

**To deactivate an existing schedule**

1 In the content area under Existing Schedules in the Existing Schedules table, click the schedule that you want to deactivate.

2 Under Plan a Schedule, uncheck Enable Schedule.

3 In the sidebar under Tasks, click Update Schedule.

The schedule appears in red in the Existing Schedules table.

4 On the toolbar, select one of the following options:

- **Save** Saves your changes.
  
  Use this option to continue making changes in the console until you are ready to apply them.

- **Apply** Applies your changes.
  
  Your changes are not implemented until you apply them.

**To activate a deactivated schedule**

1 In the content area under Existing Schedules in the Existing Schedules table, click the schedule that you want to activate.

2 Under Plan a Schedule, check Enable Schedule.
3 In the sidebar under **Tasks**, click **Update Schedule**.
The schedule appears in green in the Existing Schedules table.

4 On the toolbar, select one of the following options:

- **Save**
  Saves your changes.
  Use this option to continue making changes in the console until you are ready to apply them.

- **Apply**
  Applies your changes.
  Your changes are not implemented until you apply them.

**To delete a schedule**

1 In the content area under **Existing Schedules** in the **Existing Schedules** table, click on schedule that you want to delete.

2 In the sidebar under **Tasks**, click **Delete Schedule**.

3 On the toolbar, select one of the following options:

- **Save**
  Saves your changes.
  Use this option to continue making changes in the console until you are ready to apply them.

- **Apply**
  Applies your changes.
  Your changes are not implemented until you apply them.

See "How to monitor Symantec Protection Engine performance" on page 145.

**Monitoring Symantec Protection Engine resources**

You can monitor the resources Symantec Protection Engine uses for all of the supported protocols. If your client uses RPC, you can view the scanning threads and load statistics information for each RPC client. The RPC client must be connected to Symantec Protection Engine to appear on the Resources page.

Symantec Protection Engine refreshes the console view every 5 seconds so that you receive up-to-date information.

**Table 6-1** describes the scanning thread resources that you can monitor.
Table 6-1  Scanning threads

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RPC Client</td>
<td>IP address of the RPC client</td>
</tr>
<tr>
<td></td>
<td>This setting only applies to the RPC protocol.</td>
</tr>
<tr>
<td>Active threads</td>
<td>Number of threads that Symantec Protection Engine uses to perform the scan</td>
</tr>
<tr>
<td>Waiting threads</td>
<td>Number of threads that are available for the scanning job</td>
</tr>
<tr>
<td>Thread pool size</td>
<td>Maximum number of threads that are available for scanning</td>
</tr>
<tr>
<td></td>
<td>See “Allocating resources for Symantec Protection Engine” on page 81.</td>
</tr>
</tbody>
</table>

Table 6-2 describes the load statistics resources that you can monitor.

Table 6-2  Load statistics

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threshold for queued requests</td>
<td>Number of scan requests at which Symantec Protection Engine is at maximum load</td>
</tr>
<tr>
<td></td>
<td>See “Allocating resources for Symantec Protection Engine” on page 81.</td>
</tr>
<tr>
<td>Queued requests</td>
<td>Number of scan requests that are currently scheduled or pending</td>
</tr>
<tr>
<td>Number of requests per sec(Average over sixty seconds)</td>
<td>Average of number of scanning requests that arrived in past 60 seconds</td>
</tr>
<tr>
<td>Total files scanned(Since Installation)</td>
<td>Number of files that Symantec Protection Engine scanned since the program was installed</td>
</tr>
<tr>
<td>Total data scanned(Since Installation)</td>
<td>Total data that Symantec Protection Engine scanned since the program was installed</td>
</tr>
</tbody>
</table>

Table 6-3 describes the logging statistics resources that you can monitor.
Table 6-3 Logging statistics

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location of log files</td>
<td>Location of log files</td>
</tr>
<tr>
<td></td>
<td>See “Allocating resources for Symantec Protection Engine” on page 81.</td>
</tr>
<tr>
<td>Log directory location</td>
<td>Amount of used space for the location in which the Symantec Protection Engine logs are maintained</td>
</tr>
<tr>
<td>Used space</td>
<td>Remaining available space for the location in which the Symantec Protection Engine logs are maintained</td>
</tr>
<tr>
<td>Available space</td>
<td></td>
</tr>
</tbody>
</table>

Table 6-4 describes the Insight statistics that you can monitor.

Table 6-4 Insight statistics

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Average network query time</td>
<td>The average amount of network time (milliseconds) taken by Insight to query</td>
</tr>
<tr>
<td>Cache Hit Ratio</td>
<td>Ratio of total number of cache hits and total number of Insight queries made</td>
</tr>
</tbody>
</table>

Table 6-5 describes the miscellaneous resources that you can monitor.

Table 6-5 Miscellaneous

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process priority</td>
<td>The Symantec Protection Engine process priority</td>
</tr>
<tr>
<td></td>
<td>For more information about how to change a process priority, see the documentation for your operating system.</td>
</tr>
</tbody>
</table>

To monitor Symantec Protection Engine resources

1. In the console on the primary navigation bar, click Reports.
2. In the sidebar under Views, click Resources.

See “Enabling resource consumption logging in Symantec Protection Engine” on page 152.
Enabling resource consumption logging in Symantec Protection Engine

The Resources page on the Symantec Protection Engine console displays the information about the resources used by Symantec Protection Engine. Symantec Protection Engine refreshes the console view on the Resources page every 5 seconds so that you receive up-to-date information. From version 7.0 onwards, the data from the Resources page can now be saved in log files for further analysis. Symantec Protection Engine captures the resources data every 5 seconds and logs it every one minute. Thus, every minute 12 rows are added to the log file. The resource consumption log files are saved in the default log directory as .rcl files.

See “Enabling resource consumption logging in the Core server only mode” on page 298.

To enable resource consumption logging in Symantec Protection Engine

1. In the console on the primary navigation bar, click Monitors.
2. In the sidebar under Views, click Logging.
3. In the content area under Local Logging, check Enable resource consumption logging.
   Resource consumption logging is disabled by default.
4. In the Number of resource consumption log files to retain (one per day) box, type the number of individual log files to retain.
   The default value is 0 so that all the log files are retained or none are deleted.
5. On the toolbar, select one of the following options:
   - Save Saves your changes.
     Use this option to continue making changes in the console until you are ready to apply them.
   - Apply Applies your changes.
     Your changes are not implemented until you apply them.

See “About configuring local logging” on page 207.
See “Monitoring Symantec Protection Engine resources” on page 149.

About resource consumption log files

Resource consumption log files names have the following format.

SSE<yyyymmdd>.rcl
where, yyyy is the year, mm is the month, and dd is the day.

Table 6-6 describes the resource consumption log file content.

Table 6-6 Resource consumption log file content

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timestamp</td>
<td>Timestamp when the event was captured. The timestamp value is the offset from the standard epoch time.</td>
</tr>
<tr>
<td>No of requests per sec</td>
<td>Average of number of scanning requests that arrived in past 60 seconds.</td>
</tr>
<tr>
<td>Total files scanned till now</td>
<td>Number of files that Symantec Protection Engine scanned since the program was installed.</td>
</tr>
<tr>
<td>Total data scanned (in bytes)</td>
<td>Total data that Symantec Protection Engine scanned (in bytes) since the program was installed.</td>
</tr>
<tr>
<td>Process priority</td>
<td>The Symantec Protection Engine process priority. For more information about how to change a process priority, see the documentation for your operating system.</td>
</tr>
<tr>
<td>Used space (in bytes)</td>
<td>Amount of space (in bytes) used by the log file directory.</td>
</tr>
<tr>
<td>Available space (in bytes)</td>
<td>Amount of space available (in bytes) on the location where the log files are maintained.</td>
</tr>
<tr>
<td>Log directory location</td>
<td>Location where the log files are maintained.</td>
</tr>
<tr>
<td>RPC Client-Active</td>
<td>Details of scanning threads and load statistics for protocol configured.</td>
</tr>
<tr>
<td>Threads-Waiting</td>
<td>Example:</td>
</tr>
<tr>
<td>Threads-Thread Pool size-</td>
<td>- Log file entry for RPC protocol with a single filer configured</td>
</tr>
<tr>
<td>Threshold for queued requests-</td>
<td>198.51.100.0-0-16-128-100-0-0</td>
</tr>
<tr>
<td>Queue Requests-Number of requests(RPC)</td>
<td>- Log file entry for RPC protocol with multiple filers configured</td>
</tr>
<tr>
<td></td>
<td>198.51.100.0-0-16-128-100-0-0;203.0.113.254-0-16-128-100-0-0;...</td>
</tr>
<tr>
<td></td>
<td>For multiple RPC clients &quot;,&quot;is used as a delimiter</td>
</tr>
<tr>
<td></td>
<td>- Log file entry for ICAP protocol</td>
</tr>
<tr>
<td></td>
<td>NA-0-16-128-100-0-NA</td>
</tr>
<tr>
<td>Insight Cache Hits Ratio</td>
<td>Ratio of total number of cache hits and total number of Insight queries made.</td>
</tr>
</tbody>
</table>
### Table 6-6 Resource consumption log file content (continued)

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Insight Average Network Latency</td>
<td>The average amount of network time (milliseconds) taken by Insight to query.</td>
</tr>
</tbody>
</table>

See “Enabling resource consumption logging in Symantec Protection Engine” on page 152.

### Ways to improve Symantec Protection Engine performance

Symantec Protection Engine installs with a default configuration that is designed to balance scanning services with scanning performance. However, you can modify Symantec Protection Engine settings and resources to maximum performance.

See “Deployment considerations and recommendations” on page 154.

See “Enhance performance by limiting scanning” on page 156.

See “Configuration settings that can conserve and enhance performance” on page 163.

---

**Warning:** Before you make any modifications, carefully consider the trade offs between security and performance. For example, excluding certain files from being scanned improves overall performance. However, the files that are not scanned might contain security risks or threats that could contaminate your network if unscanned.

Ensure that you monitor performance regularly so that you can detect any degradation in performance and make the necessary adjustments as soon as possible.

See “How to monitor Symantec Protection Engine performance” on page 145.

### Deployment considerations and recommendations

Table 6-7 provides the deployment considerations that can improve Symantec Protection Engine performance.
Table 6-7 Symantec Protection Engine deployment recommendations

<table>
<thead>
<tr>
<th>Deployment consideration</th>
<th>Description</th>
</tr>
</thead>
</table>
| Determining CPU speed and system architecture capacity | Symantec Protection Engine server performance can benefit from the following features:  
- Higher CPU speed  
  CPU bottlenecks occur when Processor\%Processor Time performance counter numbers are high while the network adapter and disk I/O remain below capacity. In this case (which is the ideal CPU-maximized system), reaching 100% means that the CPU power must be increased. CPU power can be increased by upgrading to a faster CPU or by adding more processors.  
While Symantec Protection Engine can benefit from faster CPU speeds, increasing the CPU speed does not ensure a linear increase in performance. Because of the large and frequent memory access effect, an increase in CPU speed can result in wasted, idle CPU cycles when waiting for memory.  
Hyper-threading capabilities can also aid in lowering CPU utilization levels when no more than 60% of the CPU capacity is consumed. At higher CPU utilization levels, enabled hyper-threading consumes the same processing power as the disabled hyper-threading.  
- Larger processor cache  
  Large amounts of data can require frequent memory access. An L2/L3 cache improves performance when large amounts of memory are accessed.  
- Improved system architecture  
  Symantec Protection Engine transfers large data loads between network devices, memory, and the CPU. Therefore, the system elements around the CPU also have an effect on server performance. A faster memory front side bus and faster I/O buses improve overall performance. |
Table 6-7  Symantec Protection Engine deployment recommendations
(continued)

<table>
<thead>
<tr>
<th>Deployment consideration</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Determining network capacity</td>
<td>Every network device that exists on a connection has a capacity limit. Such devices include the client and server network adapters, routers, switches, and hubs that interconnect them. Adequate network capacity means that none of these network devices are saturated. You should monitor network activity to ensure that the actual loads on all network devices are below their maximum capacity. In most cases, the Internet connection bandwidth sets the limit for the volume of Internet traffic. Weak performance during peak traffic hours can be the result of over-utilization of the Internet link. If Symantec Protection Engine is connected only to LANs, you must have the proper infrastructure to support maximum traffic requirements. If the network is 1 Gbps or greater, consider enabling jumbo frames on the switch and on all of the Symantec Protection Engine servers. You should also ensure that the entire networking infrastructure is appropriately rated. For example, if you connect the computers that contain gigabit network interface cards, ensure that the network interface cards are in full duplex mode. Also ensure that the network interface cards are configured at their maximum possible bandwidth.</td>
</tr>
<tr>
<td>Determining disk storage capacity</td>
<td>Symantec Protection Engine uses disk space primarily for storing temporary files for scanning and for storing logs. A shortage of disk space might severely affect the scanning functionality of Symantec Protection Engine. If you experience disk space shortages, consider adding more physical disks.</td>
</tr>
</tbody>
</table>


Enhance performance by limiting scanning

A method that you can use to enhance scanning performance is by limiting the files that Symantec Protection Engine scans.

You can limit the files that are scanned as follows:
When you enable this option, Symantec Protection Engine scans only the file extensions or the file types that are not in the exclude lists. The default file exclude lists contain the most common file extensions and the types that are unlikely to contain threats.

See “Specifying which files to scan” on page 157.

Block the files or email messages that meet or exceed a specific size from scanning

This option lets you specify the maximum size of files or messages to scan.

See “Specifying the maximum file or message size to scan” on page 160.

Impose limits on container files

You can impose limits on how you want Symantec Protection Engine to decompose and scan container files. Imposing limits can conserve scanning resources.

You can specify the following limits for handling container files:

- The maximum amount of time, in seconds, that is spent decomposing a container file and its contents.
  
  This setting does not apply to .hqx or .amg files.

- The maximum file size, in MB, for the individual files that are in a container file.

- The maximum number of nested levels to be decomposed for scanning.

- The maximum number of bytes that are read when determining whether a file is MIME-encoded.

See “Setting container file limits” on page 161.

Specifying which files to scan

Threats are only found in the file types that contain executable code. When Symantec Protection Engine receives a top-level file or a container file, it performs an analysis of the file structure to determine its true file type. You can conserve bandwidth and time by only scanning the files that might contain threats, based upon their file extensions or file types.

Symantec Protection Engine is configured by default to scan all files regardless of extension or type.
You can choose to scan all files except those that are in the file extension and file type exclude lists. Symantec Protection Engine scans only top-level files or the files that are embedded in the archival file formats that are not contained in either list. The default exclude lists contain the most common file extensions and the file types that are unlikely to contain threats.

You can add any file extension to the File extension exclude list (file extensions must begin with a period).

The file types that you can add to the File type exclude list are as follows:

- `image/jpeg`
- `image/tiff`
- `image/x-ico`
- `audio/x-au`
- `audio/x-real`
- `audio/shn`
- `audio/x-mod`
- `video/x-msvideo`
- `binary/ms-structured-storage`
- `application/ms-tnef`
- `application/x-lha`
- `application/arj`
- `application/x-zip`
- `application/java-archive`
- `application/ani`
- `application/imz`
- `application/x-pdf`
- `application/x-zoo`

- `image/bmp`
- `image/x-png`
- `image/x-pixmap`
- `audio/mtm`
- `audio/midi`
- `audio/x-mpeg`
- `audio/x-stx`
- `audio/med`
- `video/mpeg`
- `application/x86-win-32-exe`
- `application/lzh`
- `application/rar`
- `application/x-gzip`
- `application/x-ace`
- `application/x-tar`
- `application/bh`
- `application/x-macbinary`
- `application/x-pdf`
- `application/postscript`

- `image/gif`
- `image/x-pixmap`
- `audio/x-aiff`
- `audio/x-wav`
- `audio/x-s3m`
- `audio/it`
- `video/x-ms-wmv`
- `video/quicktime`
- `application/pcx`
- `application/x-lzharc`
- `application/lz`
- `application/ole`
- `application/x-ace`
- `application/cab`
- `application/x-bz2`
- `application/x-ogg`
- `application/x-sit`
- `application/iso`
Note: Although file types are formatted similarly to MIME types, they are not derived from MIME headers of the messages that are scanned. Symantec Protection Engine derives file types by an analysis of the data itself, regardless of what information is in the MIME type.

As you evaluate which files to exclude from scanning, consider the trade-offs between performance and protection. An exclusion list lets some files bypass scanning. Thus, new types of threats might not always be detected. Scanning all files regardless of type or extension is the most secure setting, but it imposes the heaviest demand on resources. During outbreaks, you might want to scan all files even if you normally use the exclusion lists to control the files that are scanned.

Warning: Use caution if you add .jpg or .jpeg to the File extension exclude list or image/jpg, image/jpeg, or image/* to the File type exclude list. These file types can be encoded with threats and might pose a risk to your network.

To specify which files to scan

1. In the console on the primary navigation bar, click Policies.
2. In the sidebar under Views, click Scanning.
3. In the content area under Files to Scan, click Scan all files except those in the extension or type exclude lists.
4. In the File extension exclude list, do any of the following steps:
   - To add a file extension to the exclude list:
     - Type the file extension that you want to add.
     - Type each entry on a separate line. Each entry should begin with a period.
   - To remove a file extension from the exclude list:
     - Highlight and delete the file extension that you want to remove.
5 In the **File type exclude** list, do any of the following steps:

- **To add a file type to the exclude list**
  Type the file type that you want to add.
  Type each extension on a separate line. You must type the file type exactly as it appears in the list. Use the wildcard character /* to include all subtypes for a file type. For example, if you type audio/* you would exclude all audio subtypes from being scanned.

- **To remove a file type from the exclude list**
  Highlight and delete the file type that you want to remove.

6 To restore the default exclude lists, under **Tasks**, click **Reset Default List**. This option restores the default File type exclude list and File extension exclude list.

7 On the toolbar, select one of the following options:

- **Save**
  Saves your changes.
  Use this option to continue making changes in the console until you are ready to apply them.

- **Apply**
  Applies your changes.
  Your changes are not implemented until you apply them.

See “Enhance performance by limiting scanning” on page 156.

**Specifying the maximum file or message size to scan**

If your client uses the ICAP protocol, you can specify a maximum size of files or messages to scan. For messages, the maximum size includes the size of the entire message body and all attachments. For container files, the maximum size includes the container file and all of its contents. The files and mail messages that meet or exceed the maximum file size are blocked.

By default, Symantec Protection Engine has no limits on total file or message sizes.

See “Specifying the maximum file or message size to scan in the Core server only mode” on page 299.

To **specify the maximum file or message size to scan**

1 In the console on the primary navigation bar, click **Policies**.

2 In the sidebar under Views, click **Filtering**.
3 In the content area on the **Files** tab, under **Blocking by Total Message Size**, in the **Block files or messages that are larger than** box, type the maximum file size (in bytes) that Symantec Protection Engine should accept.

The default value is 0. This setting places no limits on file or message size, but internal component can handle up to 2 GB at most.

4 On the toolbar, select one of the following options:

- **Save** Saves your changes. Use this option to continue making changes in the console until you are ready to apply them.
- **Apply** Applies your changes. Your changes are not implemented until you apply them.

See “**Enhance performance by limiting scanning**” on page 156.

### Setting container file limits

Symantec Protection Engine protects your network from the file attachments that can overload the system and consume scanning performance and degrade performance.

This protection includes the container files that have any of the following characteristics:

- Overly large
- Contain large numbers of embedded, compressed files
- Are designed to maliciously use resources and degrade performance

To enhance scanning performance and reduce your exposure to denial-of-service attacks, you can impose limits to control how Symantec Protection Engine handles container files.

You can specify the following limits for handling container files:

- The maximum amount of time, in seconds, that is spent decomposing a container file and its contents
  This setting does not apply to .hqx or .amg files.
- The maximum file size, in MB, for the individual files that are in a container file
- The maximum number of nested levels to be decomposed for scanning
- The maximum number of bytes that are read when determining whether a file is MIME-encoded
Symantec Protection Engine scans a file and its contents until it reaches the maximum depth that you specify. Symantec Protection Engine stops scanning any file that meets the maximum file size limit or that exceeds the maximum amount of time to decompose. It then generates a log entry. Symantec Protection Engine resumes scanning any remaining files. This process continues until Symantec Protection Engine scans all of the files to the maximum depth (that do not meet any of the processing limits).

You can specify whether to allow or to deny access to files for which an established limit is met or exceeded. Access is denied by default.

See “Setting container file limits in the Core server only mode” on page 300.

**Warning:** If you allow access to a file that has not been fully scanned, you can expose your network to risks. If you allow access and Symantec Protection Engine detects a risk, it does not repair the file, even if under normal circumstances the file can be repaired. In this case, the file is handled as though the file is unrepairable.

---

**To set container file limits**

1. In the console on the primary navigation bar, click **Policies**.

2. In the sidebar under **Views**, click **Filtering**.

3. In the content area on the **Container Handling** tab, under **Container File Processing Limits**, in the **Time to extract file meets or exceeds** box, type the maximum time that Symantec Protection Engine can spend extracting a single container file.

   The default setting is 180 seconds (3 minutes). To disable this setting (so that no limit is imposed), type 0.

4. In the **Maximum extract size of file meets or exceeds** box, type the maximum file size, in MB, for individual files in a container file.

   The maximum value that you can specify for individual files in tar, rar, and zip containers is 30719 MB (~30 GB). The maximum value that you can specify for other containers is 1907 MB (~2 GB).

   The default setting is 100 MB. To disable this setting (so that no limit is imposed), type 0.

5. In the **Maximum extract depth of file meets or exceeds** box, type the maximum number of nested levels of files that are decomposed within a container file.

   The default setting is 10 levels. The maximum value for this setting is 50.
6 Under **NonMIME threshold**, in the **No determination after reading** box, type the maximum number of bytes that Symantec Protection Engine should scan to determine whether a file is MIME-encoded.

The default setting is 200000 bytes. If Symantec Protection Engine reads the maximum number of bytes and cannot determine whether the file is MIME-encoded, the file is considered to be non-MIME-encoded.

7 On the toolbar, select one of the following options:

- **Save** Saves your changes.
  
  Use this option to continue making changes in the console until you are ready to apply them.

- **Apply** Applies your changes.
  
  Your changes are not implemented until you apply them.

See “Enhance performance by limiting scanning” on page 156.

**Configuration settings that can conserve and enhance performance**

Table 6-8 describes the configurations that you can modify to enhance Symantec Protection Engine performance.
Table 6-8 Configurations to enhance performance

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Modify system scanning resources</td>
<td>The system scanning resource settings that you can modify to enhance performance are as follows:</td>
</tr>
<tr>
<td></td>
<td>■ Temporary directory for scanning</td>
</tr>
<tr>
<td></td>
<td>You can change the location of this temporary directory to support sites with large, specialized disk configurations. The disk space that is required for this directory varies depending on the volume of files to be scanned. Symantec Protection Engine performance depends on this directory being able to accommodate a large volume of large files during periods of peak use.</td>
</tr>
<tr>
<td></td>
<td>■ Number of available threads for scanning</td>
</tr>
<tr>
<td></td>
<td>This value defines the maximum number of scanning threads that Symantec Protection Engine generates. Symantec Protection Engine initializes the threads when the service starts. The number of threads that are initialized depends on the number of cores of the processor. The maximum value is 512 threads.</td>
</tr>
<tr>
<td></td>
<td>See “About available threads for scanning” on page 165.</td>
</tr>
<tr>
<td></td>
<td>See “Allocating resources for Symantec Protection Engine” on page 81.</td>
</tr>
</tbody>
</table>
Table 6-8 Configurations to enhance performance (continued)

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Description</th>
</tr>
</thead>
</table>
| Modify server resources                        | Symantec Protection Engine can decompose and scan the contents of container files in memory, which eliminates the latency that is imposed by on-disk scanning. This feature can improve performance in environments in which large volumes of container and archive file formats are routinely submitted for scanning. You can limit the resources that Symantec Protection Engine consumes for processing files in memory by specifying the following settings:  
  - The maximum RAM to use for the in-memory file system (in megabytes)  
    The default value is 2048 MB. The maximum value is 4096 MB (4 GB).  
    For systems with larger amounts of memory, scanning is improved when a larger section of RAM is set aside for in-memory file scanning. Keep in mind, however, that the RAM setting should be set low enough so that no file swap usage occurs.  
  - The maximum file size that can be stored within the in-memory file system (in megabytes)  
    The default setting is 256 MB. The maximum setting is 2048 MB (2 GB). Files that exceed the specified size are written to the disk.  
    This parameter defines the maximum size of a particular file which can be loaded in memory for scanning. The maximum size becomes significant if the average file size is high.  
    See “Allocating resources for Symantec Protection Engine” on page 81. |
| Notify a file server when Symantec Protection Engine updates definitions | The process of sending notifications to the file server about definition updates can affect system resources, depending on how often you schedule LiveUpdate or Rapid Release. To minimize the effect on performance, you can send the notification on demand, as needed.  
    See “Notifying a file server when definitions are updated” on page 105. |

About available threads for scanning

Symantec Protection Engine calculates the number of default threads based on the number of Cores or the processor. Symantec Protection Engine initializes the threads when the service starts. The number of threads that are initialized depends on the number of cores of the processor. The maximum value is 512 threads.
Table 6-9  Available threads

<table>
<thead>
<tr>
<th>Processor Core count</th>
<th>Min Threads</th>
<th>Max Threads</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>8</td>
<td>24</td>
</tr>
<tr>
<td>2</td>
<td>8</td>
<td>24</td>
</tr>
<tr>
<td>4</td>
<td>8</td>
<td>24</td>
</tr>
<tr>
<td>8</td>
<td>8</td>
<td>24</td>
</tr>
<tr>
<td>16</td>
<td>16</td>
<td>48</td>
</tr>
<tr>
<td>32</td>
<td>32</td>
<td>96</td>
</tr>
<tr>
<td>n&gt;=8</td>
<td>n</td>
<td>n*3</td>
</tr>
</tbody>
</table>

About telemetry data

Symantec Protection Engine sends run-time telemetry data that contains the following details to Symantec:

- Total Files Scanned
- Threats
- Files Scanned
- Total Megabytes Scanned
- Megabytes Scanned
- URLs Scanned
- URLs Blocks
- APK Reputation Violations

Symantec collects this telemetry data to know about the threats, APK violations, and blocked URLs from the overall files and URLs scanned.

The details are sent on 1st day of every month if Symantec Protection Engine is running on that day. If Symantec Protection Engine is not running on the first of the month, report for that month is not sent.
Filtering URLs

This chapter includes the following topics:

■ About filtering URLs
■ How to filter a URL
■ About URL Reputation
■ Configuring URL Reputation

About filtering URLs

If your client uses ICAP, you can filter Web sites based on Uniform Resource Locator (URL) addresses. Symantec Protection Engine uses URL categories to restrict access to the Web sites that may contain inappropriate content. You can filter outgoing requests like search engine queries and URL addresses.

Symantec Protection Engine includes the predefined URL categories that consist of URLs containing related subject matter. Symantec Protection Engine 7.0 and later is integrated with an enhanced URL database. The number of predefined URL categories have been increased following the current online trends like social networking, search engines, blogs, and online shopping. This increase in the categories lets you block access to more specific topics.

You can also create custom categories called local categories. When you place a category into the Deny Access list, access is denied to any URL that is contained in that category.

A description of the scanning modes is as follows:
Audit mode  
When you select audit mode, Symantec Protection Engine notifies the ICAP client of all the Symantec, CAIC, and Local categories that the requested URL falls under. Based on this information, the ICAP client handles the application of the filtering policies. The client determines whether to block the site and deny access.

Filtering mode  
When Symantec Protection Engine operates in the filtering mode, Symantec Protection Engine handles the application of URL filtering. You configure the types of URL that you want to deny. Based on your configuration, Symantec Protection Engine determines whether to deny access for each request. Symantec Protection Engine returns to the user an "Access Denied" message when it blocks access to a URL.

See “About the filtering modes” on page 182.
See “How to filter a URL” on page 182.

About categories
Symantec Protection Engine uses categories to determine whether access to a URL should be denied. Symantec Protection Engine provides predefined URL categories. You can also create additional categories (local categories) to meet your needs.

See “About local categories” on page 182.

About predefined URL categories
Table 7-1 provides information about the predefined URL categories that are included in Symantec Protection Engine.

<table>
<thead>
<tr>
<th>URL Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Abortion</td>
<td>Sites that provide information or arguments in favor of or against abortion; offer help to obtain or avoid abortion; describe abortion methods and how to perform them; provide testimonials on the physical, social, mental, moral, or emotional effects of abortion.</td>
</tr>
<tr>
<td>Advertising</td>
<td>Sites that provide Internet advertising services such as Sponsored ads, search engine marketing, pop-up, banner ads and so on.</td>
</tr>
</tbody>
</table>
Table 7-1  Predefined URL categories *(continued)*

<table>
<thead>
<tr>
<th>URL Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alcohol</td>
<td>Sites that promote or sell alcoholic beverages; provide recipes or techniques to make alcoholic beverages; glorify, brag, or otherwise encourage alcohol consumption or intoxication such as home brewing and distilling, recipes, clubs, and associations, and drinking games.</td>
</tr>
<tr>
<td>Anonymizer</td>
<td>Sites that offer anonymous access to Web sites through a PHP or CGI proxy, allowing users to gain access to Web sites that are blocked by corporate and school proxies as well as parental control filtering solutions.</td>
</tr>
<tr>
<td>Art and Museums</td>
<td>Sites that include art galleries, artists, and museums such as performing arts, theater, painting, drawing, sculpture, and photography are included.</td>
</tr>
<tr>
<td>Art Nudes</td>
<td>Sites that contain the non-pornographic, tasteful, and artful display of the naked body. The main purpose of these sites is not sexual arousal.</td>
</tr>
<tr>
<td>Automated Web Application</td>
<td>Sites that allow a computer to automatically open an HTTP connection for reasons such as checking for operating system or application updates.</td>
</tr>
<tr>
<td>Automotive</td>
<td>Sites that relate to manufacturers of motor vehicles, automotive dealers, motor sports, and clubs.</td>
</tr>
<tr>
<td>Bikini</td>
<td>Sites that offer the sale of bikinis, microkinis, monokinis, and thongs which are marketed as beachwear rather than swimwear. Also the sites that feature galleries and videos of models in bikinis.</td>
</tr>
<tr>
<td>Blog</td>
<td>Sites that contain ‘blogs’. Blogs are usually maintained by an individual with regular entries of commentary, descriptions of events, or other material such as graphics or video. Entries are commonly displayed in reverse chronological order like comments on specific topics, online diaries, audio and video blogs.</td>
</tr>
<tr>
<td>Business</td>
<td>Sites that are sponsored by or devoted to individual businesses and are not covered by any other categories such as aerospace and defense industries, agriculture, biotech, and chemicals.</td>
</tr>
<tr>
<td>Business Wireless</td>
<td>Sites that contain or distribute images of non-adult children that are depicted in a state of abuse. These include the sites that depict indecent images of children, advertisements for or links to such content, on a publically available Web site.</td>
</tr>
<tr>
<td>URL Category</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Cash Gambling</td>
<td>Sites that involve the wagering and exchange of money in addition to placing bets or participating in betting pools (including lotteries) online; receiving instructions, assistance or training on participating in games of chance; obtaining information, assistance or recommendations for placing a bet.</td>
</tr>
<tr>
<td>Chat</td>
<td>Sites that enable online chatting in real time. These can include text-based chat, instant messaging chat, and visual chat rooms.</td>
</tr>
<tr>
<td>Chat/SMS/Text</td>
<td></td>
</tr>
<tr>
<td>Messaging Wireless</td>
<td></td>
</tr>
<tr>
<td>Criminal Skills</td>
<td>Sites that provide instruction for threatening or violating the security of property or the privacy of people; also how to avoid complying with legally mandated duties and obligations. These include how to steal money, how to create fake IDs and documents, how to defeat locks, how to intercept phone calls, how to evade or circumvent the law.</td>
</tr>
</tbody>
</table>
### Table 7-1  Predefined URL categories (continued)

<table>
<thead>
<tr>
<th>URL Category</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Cults**    | Sites that promote prominent, organized, and modern religious groups that are identified as “cults” by three or more authoritative sources. Examples include:  
  - The Church of Satan  
  - Aum Shinrikyo  
  - The Hare Krishna movement  
  - The Family  
  - The Unification Church  
  - Branch Davidians  
  - Scientologists  |
|              | *Sources:  
  - AFF (American Family Foundation), http://www.csj.org/ - A non-profit, tax-exempt research center whose research comes from volunteer professionals ranging from fields in journalism, education, society, and law enforcement.  
  - CESNUR (Center for Studies on New Religions), http://www.cesnur.org/ - Associations of scholars working in the field of new religious movements; they operate independent of any church, denomination, or religion.  
  - University of Virginia - “Religious Movements” page, http://religiousmovements.lib.virginia.edu/profiles/listalpha.htm - A scholarly source consisting of mainly student’s research, it appears- and claims- to be one of the most current sources.  
<p>| <strong>Drugs</strong>    | Sites that promote, offer, sell, supply, encourage, or otherwise advocate the recreational or illegal use, cultivation, manufacture, or distribution of drugs, pharmaceuticals, intoxicating plants, or chemicals and their related paraphernalia. For instance, how to use recreational drugs, seeds and manufacturing tips, drug gear, and equipment. |
| <strong>Dynamic</strong>  | Sites that have dynamically changing content and may generate, display, or offer links to inappropriate material such as search engines, directory services, hosting, portals, and blogs. |
| <strong>Dynamic Wireless</strong> | |</p>
<table>
<thead>
<tr>
<th>URL Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Education</td>
<td>Sites that represent schools or other educational facilities, faculty, or alumni groups such as homeschooling, public and private schools, universities and colleges.</td>
</tr>
<tr>
<td>Energy</td>
<td>Sites that represent companies involved with the production and distribution of energy such as oil companies, gas companies, power companies, and alternative energy companies.</td>
</tr>
<tr>
<td>Enterprise Webmail</td>
<td>Sites that provide free Web email services such as Yahoo, Google, etc.; ISP email access, business, school, or institutional access by Web email, Web email provided free or paid hosting services.</td>
</tr>
<tr>
<td>Entertainment</td>
<td>Sites that relate to the entertainment industry such as official Web sites for movies, radio stations, film studios, fan sites about celebrities, and so on.</td>
</tr>
<tr>
<td>File sharing</td>
<td>Sites that provide files for downloading over the Internet or smaller private networks, through the client software to enable peer-to-peer sharing and transfer of the files.</td>
</tr>
<tr>
<td>Finance and Investing</td>
<td>Sites that provide information about personal finance and investments, investment models, guides, tips, etc. Sites that allow users online trading, buy or sell financial instruments.</td>
</tr>
<tr>
<td>Food and Restaurants</td>
<td>Sites that provide information, guides, and reviews about restaurants; specialty food shops, food recipes, and food delivery.</td>
</tr>
<tr>
<td>Forums and Message Boards</td>
<td>Sites that provide message boards and forums where users can discuss numerous topics. Sites that provide monitored or unmonitored Web forums, Bulletin boards, etc.</td>
</tr>
<tr>
<td>Freeware and Shareware</td>
<td>Sites that make software available for downloading to users such as freeware, shareware, or open source software.</td>
</tr>
<tr>
<td>Gambling</td>
<td>Sites that provide online casinos, lotteries, information and instructions about placing bets, allowing to bet online and participate in betting pools, and online Gambling.</td>
</tr>
<tr>
<td>Gaming</td>
<td>Sites that are dedicated to online games, game tips, game downloads, interactive games, and multiplayer games.</td>
</tr>
<tr>
<td>Glamour</td>
<td>Sites that promote and provide information about physical attractiveness; allure, charm, beauty, or style with respect to personal appearance, clothes, shoes, hair, make-up, and fashion accessories. Sites that contain information about Body Art and Cosmetics, hairdressing, Fashion, and Glamourous Portals.</td>
</tr>
<tr>
<td>URL Category</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Gore</td>
<td>Sites that feature graphic violence, bodily harm, or self inflicted harm. Sites that contain images of grotesque violence towards humans or animals, images of death and injury, and frightening descriptions.</td>
</tr>
<tr>
<td>Government</td>
<td>Sites that are sponsored by government branches or agencies such as Local and State Government, Health, and Social Services, Elections, Employment, Public Safety, and Services, Embassies, and Consulates.</td>
</tr>
<tr>
<td>Hacking</td>
<td>Sites that promote illegal use of technology and programming skills to access networks, databases, etc. Sites that contain techniques, skills for denial-of-service, packet sniffing, and spoofing.</td>
</tr>
<tr>
<td>Hate</td>
<td>Sites that promote hostility against particular individual or group on the basis of race, religion, color, gender, and origin.</td>
</tr>
<tr>
<td>Health</td>
<td>Sites that provide information about personal health and medical services, hygiene, diets, therapies, and counseling services about health.</td>
</tr>
<tr>
<td>Hobbies</td>
<td>Sites that provide information about personal interests like collectibles, crafts, pets, and past times.</td>
</tr>
<tr>
<td>Hosting</td>
<td>Sites that provide online systems such as free or paid hosting, dedicated or managed hosting, virtual private server hosting, and online backup file storage, to store the data.</td>
</tr>
<tr>
<td>Internet Telephony</td>
<td>Sites that provide the facility for telephone calls by Internet, or provide information or software for the purpose.</td>
</tr>
<tr>
<td>Job Search</td>
<td>Sites that are dedicated to job searches, job listings, creating and posting resumes, and organizing job fairs.</td>
</tr>
<tr>
<td>Kids</td>
<td>Sites that are dedicated to children activities such as artwork, school projects, crafts, information to answer their questions, and games.</td>
</tr>
<tr>
<td>Law</td>
<td>Sites that contain legal information about state and regional laws, lawyers, legal services, legal consultations.</td>
</tr>
</tbody>
</table>
Table 7-1  Predefined URL categories (continued)

<table>
<thead>
<tr>
<th>URL Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lifestyle</td>
<td>Sites that contain general material relevant to sexual orientation. These sites contain pages dedicated to the groups* themselves, discussions, issues, clubs, personal home pages that address or support sexual orientation lifestyle choices. These are sites mainly by target group members for target group members. Discussions and the issues that are of an explicitly mature nature are not part of this category. *The specific TARGET groups in question are gay, lesbian, bisexual, and transgender and are subsequently referred to as “GLBT”. Examples include:</td>
</tr>
<tr>
<td></td>
<td>- Sites dedicated to GLBT orientation issues, resources, outreach, portals, clubs, associations, personal sites (personal home pages), and activism.</td>
</tr>
<tr>
<td></td>
<td>- Religion, political, legal and news sources that accept, promote, or wholly address target groups. Incorporates politics (politicians and their platforms, PACs*, lobby groups); political issues (legality of gay rights, adoption, marriage, health or wellness (ACT-UP)); legal rulings or precedents.</td>
</tr>
<tr>
<td></td>
<td>- Family, adoption, or marriage or partner concerns and rights within target groups</td>
</tr>
<tr>
<td></td>
<td>- All chat pages that are devoted to GLBT issues, regardless of stated or implied chat subject(s). Gay politics chat, lesbian mothering chat, bisexual rights chat are considered as GLBT issues.</td>
</tr>
<tr>
<td></td>
<td>- GLBT advice; the sites that exclusively discuss sexual orientation issues, coming out; how to address one’s orientation with friends and family. These sites does not include these discussions that are mainly mature in nature.</td>
</tr>
<tr>
<td></td>
<td>- Transgender lifestyles by choice, cross-dressing, youth pages and “genderqueer” categories (excludes intersexual issues, that is the medical discussions, treatments, and theories surrounding children born with indeterminate genitalia); incorporates hormone therapy, elective gender reassignment, personal accounts, mental or emotional health issues and similar related items.</td>
</tr>
<tr>
<td>URL Category</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Mature Content</td>
<td>Sites that contain sexually explicit information that is not of a medical or scientific nature. These include - Discussions or descriptions of sexual techniques or exercises.</td>
</tr>
<tr>
<td></td>
<td>■ Sexual relationship counseling</td>
</tr>
<tr>
<td></td>
<td>■ Products to improve one’s sex life</td>
</tr>
<tr>
<td></td>
<td>■ Explicit discussions of sex and sexuality</td>
</tr>
<tr>
<td></td>
<td>■ Sexual orientation issues</td>
</tr>
<tr>
<td></td>
<td>■ Lingerie sales</td>
</tr>
<tr>
<td></td>
<td>■ Nudism or Naturism</td>
</tr>
<tr>
<td></td>
<td>■ Sites that refer to themselves as nudist sites, but are thinly disguised porn sites and not part of Mature Content, but are covered by the Pornography category.</td>
</tr>
<tr>
<td>Military</td>
<td>Sites that are sponsored by military branches or agencies as well as official and personal sites related to military history, ideology, or specific branches of the military.</td>
</tr>
<tr>
<td>Mobile Entertainment</td>
<td>Sites that offer a range of add-ons for handheld devices like ringtones, wallpapers, games, and videos.</td>
</tr>
<tr>
<td>Music</td>
<td>Sites that are related to the music industry such as radio Websites, band, or artist pages, music fan sites, music reviews, music studios and venues, and lyrics, tablature, and music sheet.</td>
</tr>
<tr>
<td>News</td>
<td>Sites that primarily report, inform, or comment, on current events or contemporary issues of the day. Includes sports, weather, editorials, and human interest news. Examples include:</td>
</tr>
<tr>
<td></td>
<td>■ Mainstream news services, daily news, local or regional news</td>
</tr>
<tr>
<td></td>
<td>■ Alternative news</td>
</tr>
<tr>
<td></td>
<td>■ Internet news broadcasts (audio or video)</td>
</tr>
<tr>
<td></td>
<td>■ News-oriented online and print magazines or newspapers</td>
</tr>
<tr>
<td></td>
<td>■ News services or personalized news</td>
</tr>
<tr>
<td></td>
<td>■ Editorials or opinion columns</td>
</tr>
<tr>
<td>Non profit</td>
<td>Sites that are owned by non-profit organizations. A non-profit organization (abbreviated &quot;NPO&quot;, also &quot;not-for-profit&quot;) is a legally constituted organization whose primary objective is to support or to actively engage in activities of public or private interest without any commercial or monetary profit purposes. NPOs are active in a wide range of areas, like the environment, humanitarian aid, animal protection, education, the arts, social issues, charities, health care, politics, religion, research, sports, or other endeavors.</td>
</tr>
</tbody>
</table>
Table 7-1  Predefined URL categories (*continued*)

<table>
<thead>
<tr>
<th>URL Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Occult</td>
<td>Sites that promote or offer methods, means of instruction, or other resources to affect or influence real events through the use of spells, curses, magic powers, or supernatural beings. Examples are:</td>
</tr>
<tr>
<td></td>
<td>■ Magic spells and curses, encompassing both self-defined “black” and “white” magic</td>
</tr>
<tr>
<td></td>
<td>■ Chaos Magick, Crowley, Golden Dawn, Ordo Templi Orientalis</td>
</tr>
<tr>
<td></td>
<td>■ Demonolatry (worship of demons)</td>
</tr>
<tr>
<td></td>
<td>■ Witchcraft and its practices, rituals, and activities, Wiccan magic, Pagan/neo-Pagan magic, Asatru (Odinism)</td>
</tr>
<tr>
<td></td>
<td>■ Vodun (Voodoo/Santeria)</td>
</tr>
<tr>
<td></td>
<td>■ Herbs, tools or paraphernalia for casting spells, summoning demons, or engaging in other magical behavior or activities</td>
</tr>
<tr>
<td>Personal Ads and Dating</td>
<td>Sites that promote or provide opportunity for establishing or continuing romantic or sexual relationships. Examples are:</td>
</tr>
<tr>
<td>Personal Ads and Dating Wireless</td>
<td>■ Dating portals and directories</td>
</tr>
<tr>
<td></td>
<td>■ Personal ads like general, regional, lifestyle, 900 numbers, personal pages that promote or provide personal ads</td>
</tr>
<tr>
<td></td>
<td>■ Cyber relationships</td>
</tr>
<tr>
<td></td>
<td>■ Dating portals</td>
</tr>
<tr>
<td></td>
<td>■ Directories</td>
</tr>
<tr>
<td></td>
<td>■ Cyber relationships and dating services, matchmaking services, and e-dating services</td>
</tr>
<tr>
<td></td>
<td>■ International introductions, pen pal agencies, and introduction agencies</td>
</tr>
<tr>
<td>Pets</td>
<td>Sites and forums related to the care, maintenance, purchase, rescue, or breeding of any animal for companionship and enjoyment. The category excludes livestock or laboratory animals which are kept for economic or scientific reasons. Examples include:</td>
</tr>
<tr>
<td></td>
<td>■ Pet care</td>
</tr>
<tr>
<td></td>
<td>■ Pet products</td>
</tr>
<tr>
<td></td>
<td>■ Animal rescue</td>
</tr>
<tr>
<td></td>
<td>■ Pet breeding</td>
</tr>
</tbody>
</table>
Table 7-1  Predefined URL categories (continued)

<table>
<thead>
<tr>
<th>URL Category</th>
<th>Description</th>
</tr>
</thead>
</table>
| Placeholder        | Sites that are typically owned by domain name registrars, domain brokers, or Internet advertising publishers. They usually display dynamically generated content with the intent to monetize on traffic through linked advertising listings. Examples of such sites are:  
  - Domains for sale  
  - Parked domains  
  - Expired domains  
  - Domains under construction  
  - Sites that are “coming soon” |
| Politics           | Sites that relate to politicians, election campaigns, political organizations, and publications. Includes official home pages of politicians and political parties as well as personal sites about politics and grass-root movements. |
| Pornography        | Sites that contain sexually explicit material for the purpose of arousing a sexual or prurient interest. Examples are:  
  - Sex chat rooms and portals  
  - Pornography, thumbnail or picpost sites  
  - Online pornographic magazines  
  - Pornographic picture galleries (general and topic-specific)  
  - Pornographic fiction or erotica  
  - Phone sex or live video  
  - Adult services, escort services, strippers, or mistresses  
  - Adult personal ads or Adult-themed dating services  
  - Sex toys or marital aids or videos, CD-ROMs, books, fetish clothing |
| Portal             | Sites that offer a broad array of resources and services, such as email, forums, search engines, and online shopping malls. Portals typically publish their own content or collate multiple sources of information for many areas such as news, entertainment, sports, technology, and finance. |
| Real Estate        | Sites that are commercial and involve in the real estate business. Examples are:  
  - Sites of individual brokers and agents  
  - Real estate companies  
  - Real estate search or property location services  
  - Sites offering real estate tips and advice |
<table>
<thead>
<tr>
<th>URL Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reference</td>
<td>Sites that contain personal, professional, or educational references. Examples are:</td>
</tr>
<tr>
<td></td>
<td>- Online dictionaries, encyclopedias, thesauri</td>
</tr>
<tr>
<td></td>
<td>- Maps and language translation sites</td>
</tr>
<tr>
<td>Religion</td>
<td>Sites on religion as any set of beliefs and practices that have the function of addressing the</td>
</tr>
<tr>
<td>Science</td>
<td>Sites that provide research materials in the natural and life sciences.</td>
</tr>
<tr>
<td>Search</td>
<td>Sites that support searching the Internet, newsgroups, or indices and directories.</td>
</tr>
<tr>
<td>Self Harm</td>
<td>Sites that describe or discuss ways in which to self harm including eating disorders and</td>
</tr>
<tr>
<td></td>
<td>self-injury. Eating disorders sites include:</td>
</tr>
<tr>
<td></td>
<td>- Sites about Anorexia, Bulimia, and Binge eating disorder or compulsive overeating,</td>
</tr>
<tr>
<td></td>
<td>compulsive over-exercising, pica, prader-willi syndrome, night eating syndrome, body</td>
</tr>
<tr>
<td></td>
<td>dysmorphic disorder, othorexia, and bigorexia</td>
</tr>
<tr>
<td></td>
<td>- Sites supporting eating disorder as a lifestyle choice covering issues like diet and</td>
</tr>
<tr>
<td></td>
<td>exercise methods, how to hide your eating disorder, the thin commandments, and so on.</td>
</tr>
<tr>
<td></td>
<td>- Personal pages, journals, blogs, forums, webrings supporting an eating disorder lifestyle</td>
</tr>
<tr>
<td></td>
<td>- Picture pages or galleries created for inspiring people with eating disorders, for example,</td>
</tr>
<tr>
<td></td>
<td>thinspiration, thinspo.</td>
</tr>
<tr>
<td></td>
<td>Self-injury sites include:</td>
</tr>
<tr>
<td></td>
<td>- Sites about self-injury including cutting, punching, hitting, scratching, choking,</td>
</tr>
<tr>
<td></td>
<td>self-biting, picking at wounds, and self-poisoning.</td>
</tr>
<tr>
<td></td>
<td>- Personal pages, forums, and clubs that may trigger self-injurious behavior</td>
</tr>
<tr>
<td></td>
<td>- Self injury webrings</td>
</tr>
<tr>
<td></td>
<td>- Pictures of self injury</td>
</tr>
<tr>
<td>Sexual</td>
<td>Sites that provide educational information on reproduction and sexual development,</td>
</tr>
<tr>
<td>Education</td>
<td>sexually transmitted disease, contraception, safe sexual practices, sexuality, and sexual</td>
</tr>
<tr>
<td></td>
<td>orientation.</td>
</tr>
<tr>
<td>URL Category</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Shopping</strong></td>
<td>Sites that provide the means to purchase products or services online. Products or services that are principally marketed to satisfy industrial or commercial needs are not included in this category. Examples are:</td>
</tr>
</tbody>
</table>
|                  | ▪ Pages offering an item intended for personal usage for sale, with price, description, order number, or some combination thereof  
|                  | ▪ Internet malls  
|                  | ▪ Online auctions  
|                  | ▪ Department or retail stores online catalogs  
|                  | ▪ Services that are meant to benefit the private individual                                                                                                                                           |
| **Sports**       | Sites that promote or provide information about spectator sports. Examples are:                                                                                                                                 |
| **Sports Wireless** | Professional sports teams, leagues, organizations, or association sites; player and fan sites  
|                  | Collegiate football, basketball, etc.; men's and women's; team, league, and conference sites; player and fan sites  
|                  | Sites for official Olympic Committees; media Olympic portals  
|                  | Sports portals and directories - scores, schedules, news, statistics, discussion, etc.; spectator sports link aggregations  
|                  | Sports event ticket sales for targeted professional or collegiate sports; sports tourism  
|                  | Online magazines, newsletters, chats, and forums for targeted professional and collegiate sports                                                                                                          |
| **Streaming Media** | Sites that host streaming media like television, movies, video, radio, or other media.                                                                                                                     |
| **Suicide**      | Sites that describe or promote suicide. Examples are:                                                                                                                                                      |
|                  | ▪ Suggestions on how to kill yourself; newsgroups; chat rooms; message boards  
|                  | ▪ Descriptions or depictions of methods, systems, or machines; instructions  
|                  | ▪ Personal stories; suicide diaries; blogs; forums  
|                  | ▪ Famous suicides or details of famous suicides  
|                  | ▪ Famous suicide spots  
|                  | ▪ Glorification or worshipful attitude to suicide
<table>
<thead>
<tr>
<th>URL Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technology and Telecommunications</td>
<td>Sites that provide information pertaining to computers, the Internet as well as telecommunication. Examples are:</td>
</tr>
<tr>
<td></td>
<td>- Software solutions and services</td>
</tr>
<tr>
<td></td>
<td>- Computer and telecommunication hardware, devices, and gadgets</td>
</tr>
<tr>
<td></td>
<td>- Internet and phone access services</td>
</tr>
<tr>
<td></td>
<td>- Technology news</td>
</tr>
<tr>
<td>Tobacco</td>
<td>Sites that encourage, promote, offer for sale or otherwise encourage the consumption of tobacco. Examples are:</td>
</tr>
<tr>
<td></td>
<td>- Retailers and manufacturers from the tobacco industry</td>
</tr>
<tr>
<td></td>
<td>- Tobacco products and paraphernalia</td>
</tr>
<tr>
<td></td>
<td>- Smoking is good, glamorous, or cool</td>
</tr>
<tr>
<td></td>
<td>- How to smoke or smoking lessons</td>
</tr>
<tr>
<td>Travel</td>
<td>Sites that promote or provide opportunity for travel planning in a general sense, particularly finding, and making travel reservations. Examples are:</td>
</tr>
<tr>
<td>Travel Wireless</td>
<td>- Travel portals, packages, and information (includes tours, travel clubs and associations, and travel information for specific demographic groups)</td>
</tr>
<tr>
<td></td>
<td>- Air travel (air carriers: tickets/reservations/charters)</td>
</tr>
<tr>
<td></td>
<td>- Sites that facilitate travel-related transportation (tickets/reservations/charters/rentals of trains, buses, boats, motorcycles. Does not include car rentals.)</td>
</tr>
<tr>
<td></td>
<td>- Lodging (includes lodging directories and portals)</td>
</tr>
<tr>
<td></td>
<td>- Travel agents and travel auctions</td>
</tr>
<tr>
<td>Violence</td>
<td>Sites that advocate or provide instructions to cause physical harm to people or property through use of weapons, explosives, pranks, or other types of violence. Examples are:</td>
</tr>
<tr>
<td></td>
<td>- Explosives and bombs: How to manufacture, obtain materials, transport, or seed an area, including but not limited to making explosives using common household items.</td>
</tr>
<tr>
<td></td>
<td>- Pranks, destructive mischief, &quot;revenge,&quot; teenage anarchy including but not limited to dangerous chemistry</td>
</tr>
<tr>
<td></td>
<td>- Descriptions or instructions for killing people</td>
</tr>
</tbody>
</table>
### Table 7-1 Predefined URL categories (continued)

<table>
<thead>
<tr>
<th>URL Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Community</td>
<td>Sites that offer a variety of tools and mechanisms to enable a group of people to communicate and interact by the Internet. Examples include:</td>
</tr>
<tr>
<td></td>
<td>■ Social networking</td>
</tr>
<tr>
<td></td>
<td>■ Chat and instant messaging</td>
</tr>
<tr>
<td></td>
<td>■ Forums &amp; Messageboards</td>
</tr>
<tr>
<td></td>
<td>■ Hosting of home pages and other user generated content including audio and video</td>
</tr>
<tr>
<td>Weapons</td>
<td>Sites that describe or offer for sale weapons including guns, ammunition, firearm accessories, knives, and martial arts. Examples are:</td>
</tr>
<tr>
<td></td>
<td>■ Online sales of firearms, ammunition, accessories, and knives</td>
</tr>
<tr>
<td></td>
<td>■ Descriptions, reviews, specifications, or weapons</td>
</tr>
<tr>
<td></td>
<td>■ Weapons retailers, manufacturers, auctions, and trading centers</td>
</tr>
<tr>
<td></td>
<td>■ Instructions for manufacture of weapons</td>
</tr>
<tr>
<td>Webmail</td>
<td>Sites that provide Web based email services that are freely available and accessible through any Internet browser.</td>
</tr>
<tr>
<td>Wedding</td>
<td>Sites related to the traditions, customs, planning, and products involved in a marriage or commitment ceremony as well as in civil unions.</td>
</tr>
<tr>
<td></td>
<td>■ Wedding planning</td>
</tr>
<tr>
<td></td>
<td>■ Wedding products</td>
</tr>
<tr>
<td></td>
<td>■ Alternative commitment ceremonies</td>
</tr>
</tbody>
</table>

Symantec periodically updates the predefined URL categories. Symantec Protection Engine automatically downloads updated categories through LiveUpdate. Symantec might create new URL categories to address additional content areas as needed. New categories are not active by default. You must select the new categories that you want to use for URL blocking.

The predefined URL categories cannot be modified.

See “Overriding a URL categorization” on page 189.

**Note:** If the requested URL belongs to the CAIC category, the URL is replaced with the text CAIC-URL in all the corresponding messages and logs.

See “About categories” on page 168.
About local categories

You can create your own custom categories. Categories that you create are called local categories. Access to the URLs that you add to local categories is denied by default. To turn off a local category, you must change the category configuration.

See “Managing local categories” on page 185.

How to filter a URL

If your client uses ICAP, you can take advantage of the URL filtering capabilities of Symantec Protection Engine. You must have the appropriate URL filtering licenses to use the URL filtering features in Symantec Protection Engine.

See “About licensing” on page 88.

You can configure URL filtering by taking any of the following steps:

- Enable URL filtering and select the appropriate filtering mode.
  See “Enabling URL filtering in Symantec Protection Engine” on page 183.
  See “About the filtering modes” on page 182.

- Specify the URLs (by subject content) to which you want to deny access.
  See “Denying access to URLs in URL categories” on page 184.

- Create and populate local categories with sites to which you want to deny user access.
  See “Managing local categories” on page 185.

- Override URL categorizations by adding URLs to Allow categories.
  See “Overriding a URL categorization” on page 189.

- Customize the "Access Denied" message that users see when access to a URL is denied.
  See “Customizing the access denied message” on page 190.

About the filtering modes

Symantec Protection Engine lets you scan URLs in audit mode or the filtering mode. The mode that you use depends on the capabilities of the client application for which Symantec Protection Engine provides URL filtering. It also depends on the manner in which Symantec Protection Engine is deployed.

Note: When you change from audit mode to the filtering mode, the URL category and local category settings revert to settings that you configured (and applied) in the filtering mode.
About filtering mode in Symantec Protection Engine

When Symantec Protection Engine operates in the filtering mode, Symantec Protection Engine handles URL filtering and the denial-of-access to restricted sites.

Specify the categories to deny. Based on your configuration, Symantec Protection Engine determines whether to deny access for each request. If access is denied, Symantec Protection Engine returns an "Access Denied" message to the user.

See “Customizing the access denied message” on page 190.

When Symantec Protection Engine scans in the filtering mode, it stops scanning when the first URL match is found.

About audit mode in Symantec Protection Engine

When Symantec Protection Engine operates in audit mode, the ICAP client handles the application of URL filtering and the denial-of-access to restricted sites.

Symantec Protection Engine provides the ICAP client with the information that is necessary to determine whether a site should be blocked. The client decides how the request is handled.

When you select audit mode, all URL categories and local categories are automatically included in the Audit list. You cannot select specific categories to include in the Audit list. However, you can add and delete local categories.

See “Managing local categories” on page 185.

For each request from the ICAP client, Symantec Protection Engine matches the request against all categories. Symantec Protection Engine notifies the client if the requested URL is contained in any URL category or local category. Based on the information that Symantec Protection Engine returns, the ICAP client determines whether the site should be blocked.

When Symantec Protection Engine scans in audit mode, scanning does not stop when a single URL match is found. It continues to scan against all categories. Symantec Protection Engine provides the results to the ICAP client so that it has all of the information it needs to handle the request.

Enabling URL filtering in Symantec Protection Engine

Symantec Protection Engine is provided with minimum URL definitions. We recommend you to run LiveUpdate and update the URL definitions before you start URL filtering.

URL filtering can be enabled during installation. If you did not enable URL filtering during installation, follow the steps below to enable it.

See “Enabling URL filtering in the Core server only mode ” on page 303.
To enable URL filtering

1. In the console on the primary navigation bar, click **Policies**.
2. In the sidebar under **Views**, click **Filtering**.
3. On the **URL** tab, under **URL Filtering**, select **Enable URL Filtering and download URL Filtering definitions**.
4. Under **Enable URL Filtering and download URL Filtering definitions**, select **Filtering mode** or **Audit mode**.
5. On the toolbar, select one of the following options:
   - **Save**: Saves your changes. Use this option to continue making changes in the console until you are ready to apply them.
   - **Apply**: Applies your changes. Your changes are not implemented until you apply them.

Denying access to URLs in URL categories

Symantec Protection Engine includes predefined URL categories. URL categories consist of URLs that contain related subject matter. You can deny access to URLs when you add the category to the Deny Access list. When you deny access to a URL category, access to the URLs that are contained in that category is denied. However, you can override the categorization of a URL.

See "Denying access to URLs in URL categories in the Core server only mode" on page 304.

See “Overriding a URL categorization” on page 189.

**Note**: Symantec Protection Engine automatically encodes and saves the text strings in Unicode/UTF-8 when you apply your changes in the console.

None of the URL categories are in the **Deny Access** list and access to the URLs in every category is permitted by default. You must select the URL categories that you want to add to the **Deny Access** list.

To deny access to URL categories

1. In the console on the primary navigation bar, click **Policies**.
2. In the sidebar under **Views**, click **Filtering**.
3 On the URL tab, under **URL Filtering**, select **Enable URL Filtering and download URL Filtering definitions**.

4 Under **Configure Categories**, select **Deny Access** for each URL category for which you want to deny access.

5 On the toolbar, select one of the following options:

- **Save** Saves your changes.
  - Use this option to continue making changes in the console until you are ready to apply them.

- **Apply** Applies your changes.
  - Your changes are not implemented until you apply them.

**Managing local categories**

You can create your own custom categories. Categories that you create are called local categories. You can use local categories to deny access to sites that have not been categorized in one of the predefined URL categories. Access is denied to the URLs that are associated with the local categories and are in the Deny Access list.

Local categories are denied by default (that is, they are in the Deny Access list). To permit access to URLs in a local category, you must change the category configuration.

When you add URLs to a local category, you can be as specific or as general as you want. Symantec Protection Engine looks for the most exact match when a URL is checked. Based on the entry in a category, you can block or allow individual Web pages or entire directories, computers, or domains.

**Table 7-2** provides examples of how you can vary the URLs that you enter in the categories to provide general or specific blocking.

<table>
<thead>
<tr>
<th>Filtered URL</th>
<th>Effect</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://www.symantecexample.com/pics/apr.html">www.symantecexample.com/pics/apr.html</a></td>
<td>Matches this one specific page</td>
</tr>
<tr>
<td><a href="http://www.symantecexample.com/pics">www.symantecexample.com/pics</a></td>
<td>Matches the entire directory</td>
</tr>
<tr>
<td><a href="http://www.symantecexample.com">www.symantecexample.com</a></td>
<td>Matches this computer</td>
</tr>
<tr>
<td>symantecexample.com</td>
<td>Matches the entire domain</td>
</tr>
</tbody>
</table>
For example, if you add the domain symantecexample.com to a denied category, access to all URLs in that domain is denied. If you want to deny access to one of the URLs within that domain, add a more specific URL to one of the local categories. For example, www.symantecexample.com/daily-news. Because Symantec Protection Engine looks for the most exact match, access to the specific URL is allowed. Access is denied to any other content from that domain.

Note: You cannot allow or deny access to a URL based on Internet protocol (for example, HTTP, FTP, and HTTPS). When you add a URL to a local category and deny access to that category, all connections are uniformly blocked.

You can manage local categories as follows:

- Create a local category.
  You can create up to 256 local categories.
- Delete a local category.
- Add a URL to a local category.
  Use host names rather than IP addresses.
- Delete a URL from a local category.

To create a local category

1. In the console on the primary navigation bar, click Policies.
2. In the sidebar under Views, click Filtering.
3. On the URL tab, under URL Filtering, select Enable URL Filtering and download URL Filtering definitions.
4. Under Tasks, click Add Local Category.

   In the content area on the URL tab, under Local Categories, the new category displays in the list of local categories. The category is temporarily called: rename.
5 Type a new name for the category.

Categories can be up to 64 characters in length. Category names are not case-sensitive.

Local categories are denied by default.

6 On the toolbar, select one of the following options:

- **Save**: Saves your changes.
  Use this option to continue making changes in the console until you are ready to apply them.

- **Apply**: Applies your changes.
  Your changes are not implemented until you apply them.

To delete a local category

1 On the URL tab, under **URL Filtering**, select **Enable URL Filtering and download URL Filtering definitions**.

2 Under **Local Categories**, select the category you want to delete from the list of local categories.

3 In the sidebar under **Tasks**, click **Delete Local Category**.

4 On the toolbar, select one of the following options:

- **Save**: Saves your changes.
  Use this option to continue making changes in the console until you are ready to apply them.

- **Apply**: Applies your changes.
  Your changes are not implemented until you apply them.

To add a URL to a local category

1 On the URL tab, under **URL Filtering**, select **Enable URL Filtering and download URL Filtering definitions**.

2 Under **Local Categories**, select the category to which you want to add a URL from the list of local categories.
3 In the **URLs associated with selected Local Category (maximum 999 characters per URL)** box, type the URL that you want to add.

   Type one URL per line. You can enter maximum 999 characters per URL.

4 On the toolbar, select one of the following options:

   - **Save**
     - Saves your changes.
     - Use this option to continue making changes in the console until you are ready to apply them.

   - **Apply**
     - Applies your changes.
     - Your changes are not implemented until you apply them.

**To delete a URL from a local category**

1 On the **URL** tab, under **URL Filtering**, select **Enable URL Filtering and download URL Filtering definitions**.

2 Under **Local Categories**, select the local category from which you want to delete a URL.

   The URLs that are contained in the selected category are displayed in the **URLs associated with selected Local Category (maximum 999 characters per URL)** box.

3 In the **URLs associated with selected Local Category (maximum 999 characters per URL)** box, highlight the URL that you want to remove, and then press **Delete**.

4 On the toolbar, select one of the following options:

   - **Save**
     - Saves your changes.
     - Use this option to continue making changes in the console until you are ready to apply them.

   - **Apply**
     - Applies your changes.
     - Your changes are not implemented until you apply them.

See “**About filtering URLs**” on page 167.

See “**About categories**” on page 168.
Overriding a URL categorization

You can override the categorization of a URL in a predefined URL category by adding the URL to the URL List Override. URLs that are contained in the URL List Override are always permitted.

When a URL request is submitted, Symantec Protection Engine checks the URL List Override before it checks the categories in the Deny Access list. If it finds a match in the URL List Override, it does not check the Deny Access list categories. The URL List Override functions in the same manner for both audit and filtering mode.

Add only the URLs to the URL List Override that you know contain acceptable material. When you place a URL in the URL List Override, you permit unconditional access to the URL.

---

**Note:** You cannot allow or deny access to a URL based on Internet protocol (for example, HTTP, FTP, and HTTPS). When a URL is contained in a local category that is in the Deny Access list, all connections are uniformly blocked.

---

**To override a URL categorization**

1. In the console on the primary navigation bar, click **Policies**.
2. In the sidebar under **Views**, click **Filtering**.
3. On the **URL** tab, under **URL Filtering**, select **Enable URL Filtering and download URL Filtering definitions**.
4. Under **URL List Override (maximum 999 characters per URL)**, type the URL for which you want to allow access.
   - Type one URL per line. You can enter maximum 999 characters per URL.
5. On the toolbar, select one of the following options:
   - **Save** Saves your changes.
     - Use this option to continue making changes in the console until you are ready to apply them.
   - **Apply** Applies your changes.
     - Your changes are not implemented until you apply them.

See “**About filtering URLs**” on page 167.
Customizing the access denied message

Symantec Protection Engine displays an Access denied message to the user when access to a Web site is blocked. The default message is as follows:

Access to the destination `${URL_REQUESTED}` is prohibited. `${REASON}`

You can customize the message using the following variables:

- `${URL_REQUESTED}`: The URL address that the user requested.
- `${REASON}`: An explanation of why the URL address that the user requests is blocked.

When a Web site is blocked due to URL violation, the `${REASON}` variable reads as follows:

- Found in denied list `<(category)>`

where `<(category)>` is the URL or local category that contains the URL that is denied.

See “Customizing the access denied message in the Core server only mode” on page 304.

To customize the access denied message

1. In the console on the primary navigation bar, click **Policies**.
2. In the sidebar under **Views**, click **Filtering**.
3. On the **URL** tab, under **URL Filtering**, select **Enable URL Filtering and download URL Filtering definitions**.
4. Under **Access Denied Message**, customize the user notification message.
5. On the toolbar, select one of the following options:

   - **Save**: Saves your changes. Use this option to continue making changes in the console until you are ready to apply them.
   - **Apply**: Applies your changes. Your changes are not implemented until you apply them.

See “How to filter a URL” on page 182.
About URL Reputation

URL Reputation feature identifies threats from domains and URLs, which can be hosting malicious content like malware, fraud, phishing, and spam etc. The URL Reputation feature lets you block access to the web addresses that are identified as known sources of the malicious content.

The URL Reputation feature restricts access to the URLs and domain based on the reputation and confidence level. Symantec assigns confidence and reputation ratings to each identified web address. You can choose threshold settings for these ratings as per your requirements. Confidence is a measure of how sure we are of the validity of the information and reports. Confidence is rated on a 1 to 5 scale, where 1 is the baseline confidence and 5 is a very high confidence. Reputation takes into account all domain/URL-specific and behavior-specific ratings. The Reputation is rated is on a scale of 1 to 10. Where 1 is the baseline reputation required for inclusion in the feed and 10 is the worst possible reputation.

URL Reputation definitions can be updated using Symantec LiveUpdate mechanism. See “Configuring URL Reputation” on page 191.

See “Configuring the additional parameters of URL Reputation” on page 391.

Configuring URL Reputation

The URL Reputation feature is disabled by default. You must enable it and configure the additional parameters as per your requirements.

To configure URL Reputation

1. In the console on the primary navigation bar, click Policies.
2. In the sidebar under Views, click Filtering.
3. On the URL tab, under URL Reputation, select Enable URL Reputation and download URL Reputation definitions.
4. Select the URL reputation level from the Reputation list.

Reputation level is the value that provides information on how bad the Domain/URL is. This level is dynamic in nature and can vary with definitions update.
5 Select the URL confidence level from the Confidence list.

Confidence is a measure of how confident Symantec is of the validity of the information and reports. This value is dynamic in nature and can vary with definitions update.

6 On the toolbar, select one of the following options:

Save

Saves your changes.

Use this option to continue making changes in the console until you are ready to apply them.

Apply

Applies your changes.

Your changes are not implemented until you apply them.
Android Application (APK) Reputation

This chapter includes the following topics:

- About Android Application (APK) Reputation
- Configuring the APK Reputation

About Android Application (APK) Reputation

Symantec Protection Engine lets you classify untrusted APK files by using APK Reputation feature. APK Reputation uses Symantec’s mobile intelligence framework that leverages the data from a number of sources.

Symantec Protection Engine currently supports APK reputation scanning by using true type detection of the APK files. Symantec Protection Engine uses the security rating that is provided by the reputation server to allow, block, or delete an APK file.

Symantec Protection Engine exposes security rating on a scale of 0 to 6. Where 0 is the best security rating that can be assigned to an APK file and 6 is the worst possible security rating. Rating 3 denotes “NEUTRAL” security rating.

APK files are allowed, blocked, or deleted based on the value that is configured in Symantec Protection Engine. APK files that have security rating greater than or equal to the configured value can be blocked or deleted. You can also quarantine such files for further analysis. APK files that have security rating lower than the configured value are allowed.

Symantec Protection Engine caches the security ratings of the APK files. The duration for which the entry remains in cache is determined by configured time to live. If configured time to live for cache is 0, then the duration is determined by the security rating of an APK file as mentioned in the following table:
Table 8-1  Cache duration of security rating

<table>
<thead>
<tr>
<th>Time to live</th>
<th>Security rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>14 days</td>
<td>High Good and High Bad</td>
</tr>
<tr>
<td>7 days</td>
<td>Medium Good and Medium Bad</td>
</tr>
<tr>
<td>3 days</td>
<td>Low Good and Low Bad</td>
</tr>
<tr>
<td>1 day</td>
<td>Neutral and partially processed APK file</td>
</tr>
</tbody>
</table>

This cache is saved to the hard disc after the configured interval of time.

See “Configuring APK Reputation in the Core server only mode” on page 267.
See “Configure the additional parameters of APK Reputation” on page 390.

Configuring the APK Reputation

APK Reputation feature is enabled by default. You can configure threshold security rating and action policy settings on Symantec Protection Engine console.

To configure the APK Reputation

1 In the console on the primary navigation bar, click **Policies**.
2 In the sidebar under **Views**, click **APK Reputation**.
3 In the content area under **Android Application (APK) Reputation**, select **Enable APK Reputation** to enable the feature.
4 Select one of the following options:
   - **Block**: Blocks the APK file if the security rating is above or equal to the configured threshold value.
   - **Delete**: Deletes the APK file if the security rating is above or equal to the configured threshold value.
5 Select one of the following ratings from the **Threshold security rating** list:
   - High Good
   - Medium Good
   - Low Good
   - Neutral
   - Low Bad
   - Medium Bad
High Bad

6 In the **Avoid APK scanning for files larger than** box, specify the file size in bytes to exclude the file from APK Reputation scanning.

7 On the toolbar, select one of the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Save</td>
<td>Saves your changes. Use this option to continue making changes in the console until you are ready to apply them.</td>
</tr>
<tr>
<td>Apply</td>
<td>Applies your changes. Your changes are not implemented until you apply them.</td>
</tr>
</tbody>
</table>

See “About Android Application (APK) Reputation” on page 193.

See “Configure the additional parameters of APK Reputation” on page 390.
Traffic monitor mode in Symantec Protection Engine

This chapter includes the following topics:

- About traffic monitor mode in Symantec Protection Engine
- Functional changes in Symantec Protection Engine
- About traffic statistics summary collection:
  - About traffic statistics collection
  - Configuring Symantec Protection Engine to function in Traffic monitor mode

About traffic monitor mode in Symantec Protection Engine

Symantec Protection Engine is now incorporated with a new mode that monitors the scan requests. In this mode, Symantec Protection Engine is configured in RPC mode to collect different traffic statistics during the specified time period.

In this mode, Symantec Protection Engine does not scan the files. It only collects the different file statistics such as file size, file extension, maximum file size, minimum file size, average file size and average number of requests along with some other parameters. This mode collects the traffic statistics, which helps in deciding the sizing of the customer environment.

Following are the two modes of traffic monitoring in Symantec Protection Engine:

ENABLE_TRAFFIC_MONITOR_MODE:

This environment variable decides whether traffic monitor mode is enabled or not in Symantec Protection Engine. When the value is set to 1, Symantec Protection
Engine functions in traffic monitor and only collects different file statistics. Any value other than 1, indicates that the traffic monitor mode is disabled. In this scenario, Symantec Protection Engine functions normally as it currently does. To enable traffic monitor mode, setting the environment variable value to 1 is mandatory.

**TRAFMON_SUMMARY_COLLECT_INTERVAL:**

This environment variable, helps decide the time interval in which traffic statistics needs to be collected and logged to summary statistics file. The value of this environment variable should be an unsigned number. The minimum allowed value is 1 and the maximum allowed value is 240. Unit of these values is hour. Summary collection time interval value is allowed from a minimum of 1 hour to a maximum of 240 hours (10 days). The default value of this parameter is 1 hour. This variable is an optional environment variable and if not set, Symantec Protection Engine treats the default value as 1 hour.

If any value that is less than 1 is provided then Symantec Protection Engine sets the value to 1 hour. If any value that is more than 240 is provided then its value is set to 240 hours.

### Functional changes in Symantec Protection Engine

When traffic monitor mode is enabled, Symantec Protection Engine, generates two additional logs. Name format of these logs are:

- SSEYYYYMMDD.tdat
- SSEYYYYMMDD.stdat

In traffic monitor mode, Symantec Protection Engine does not generate the normal statistics file (SSEYYYYMMDD.dat) as most of the parameters in this mode are of no use as there is no actual scanning occurring.

Traffic statistics gets generated either at configured time interval or when Symantec Protection Engine is shutdown.

### About traffic statistics summary collection:

Traffic statistics summary collection occurs after every hour that is configured through TRAFMON_SUMMARY_COLLECT_INTERVAL environment variable. The default time considered is 1 hour.

The file name format for traffic statistics summary collection file is SSEYYYYMMDD.stdat. The header that is used in this file is displayed as follows:

- Time, Start time, End time, Total requests count, Total file size in MB, Maximum file size in MB, Minimum file size in MB, Average file size
In traffic monitor mode, Symantec Protection Engine reads the list of all file extensions from file_extension_list.conf configuration file and creates the above mentioned header dynamically. You can configure the desired file extension in file_extension_list.conf configuration file, if it is not present there. Each line must list one extension.

By default there is a list of 50 file extensions present in this file. User can configure a maximum of 200 such extensions in this configuration file. If user configures more than 200 files then the top 200 extensions are read and inserted in the header. Remaining extensions are ignored. There are two special extensions headers no_extension and other is always present in the extension list of header. If there is a file without extension in the request then such a file is counted under no_extension header column. If there is a file having an extension that is not present in any of the configured extension lists in the header then all such files are counted under another field of the header.

About traffic statistics collection

Traffic statistics collection occurs every one minute. File name format for traffic statistics file is displayed as SSEYYYYYMMDD.tdat. The header that is used in this file looks like the following:

Time, Total requests count, Total file size in MB, Maximum file size in MB, Minimum file size in MB, Average file size in MB, Request throughput (MBps), Number of files (0-3 MB), Number of files (>3-7 MB), Number of files (>7-11 MB), Number of files (>11-20 MB), Number of files (>20-50 MB), Number of files (>50-100 MB), Number of files (>100-200 MB), Number of files (>200-500 MB), Number of files (>500-1024 MB), Number of files (>1024-2048 MB), Number of files (>2048 MB)

Header represents all the fields that are logged in this file.
Configuring Symantec Protection Engine to function in Traffic monitor mode

To enable traffic monitor mode in Symantec Protection Engine:

1. Go to advanced system settings on your machine and set the environment variable as ENABLE_TRAFFIC_MONITOR_MODE and TRAFMON_SUMMARY_COLLECT_INTERVAL.

   The ENABLE_TRAFFIC_MONITOR_MODE is mandatory and the TRAFMON_SUMMARY_COLLECT_INTERVAL is optional.

2. Install Symantec Protection Engine (SPE) and make changes in configuration.xml and set the protocol as ‘RPC’ and filer IP configuration.

3. Configure Symantec Protection Engine service to run with proper Active Directory credentials as required to run with 7G or C-mode filer.

4. Configure the 7G or C-mode filer as per specification.

5. Restart the Symantec Protection Engine service.
Logging data, issuing alerts, and generating reports

This chapter includes the following topics:

- About logging data
- About configuring local logging
- Configuring logging to the Windows Application Event Log
- Configuring logging to the Linux Syslog
- About configuring alerts
- About reports

About logging data

Symantec Protection Engine provides several logging and alert destinations. You can activate logging to each available destination by selecting a logging level that you want for that destination. You can then choose the types of events for which log messages are generated. For each logging destination that you choose, you can select a different logging level.

See “Logging destinations” on page 200.

See “Logging levels and events” on page 202.

Logging destinations

Table 10-1 shows the destinations to which Symantec Protection Engine can forward log events.
### Table 10-1 Logging destinations

<table>
<thead>
<tr>
<th>Destination</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local logs</td>
<td>Symantec Protection Engine logs events to the local logs by default. The default location for the local logs for Linux is /opt/SYMCScan/log. The default location for the local logs for Windows platform C:\Program Files\Symantec\Scan Engine\log. You can change the location of the logs. You can use the reporting functions to view the local logs. See “About configuring local logging” on page 207.</td>
</tr>
<tr>
<td>Windows Application Event Log</td>
<td>If you are running Symantec Protection Engine on Windows, you can log events to the Windows Application Event Log. See “Configuring logging to the Windows Application Event Log” on page 212.</td>
</tr>
</tbody>
</table>
| Statistics logs                                  | Statistics logs are used to report the following cumulative scan data:  
  - Total number of files that are scanned, repaired, and quarantined  
  - Total megabytes scanned  
  - Types of violations that are found by violation type  
  You must enable logging to the statistics logs so that you can view statistics reports. Scan data is logged daily to the statistics log files. You can use the reporting functions to view the statistics data. See “Enabling statistics reporting in Symantec Protection Engine” on page 211. |
| RPC client logging subsystem (RPC only)           | If your client uses RPC, Symantec Protection Engine logs certain events to the RPC client logging subsystem. Logging to the RPC client is in addition to the other logging destinations that are available. See “Logging to the RPC client logging subsystem” on page 107. |
| Abort log                                        | Information is logged to the abort log only when Symantec Protection Engine fails to start before the standard protection engine logging is initiated. This failure can occur, for example, if the XML does not validate. If this failure occurs, information about the failure is written to the abort log file, SymantecProtectionEngineAbortLog.txt. This file is located in the installation directory. |
Table 10-1  Logging destinations (continued)

<table>
<thead>
<tr>
<th>Destination</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Center Operations Manager</td>
<td>You can integrate Symantec Protection Engine events with System Center Operations Manager (SCOM). System Center Operations Manager is a central repository that can receive critical events, errors, warnings, and other information from your Symantec Protection Engine servers. Preconfigured rules are automatically created when you import the management pack. These rules monitor specific Symantec Protection Engine events in the Windows Event Log. When a rule is triggered, the Operations Manager 2007 Agent collects data about the event and forwards it to the System Center Operations Manager. For more information, see the Symantec™ Protection Engine Management Pack Integration Guide in the Symantec_Protection_Engine_Tools.zip file. Tools\SCOM\Docs\SPE_Management_Pack_Integration_Guide.pdf</td>
</tr>
</tbody>
</table>

Logging levels and events

You can select a different logging level for each logging and alert notification destination. For example, Symantec Protection Engine can log Error logging level events to the local log. It can log Warning logging level events to the Windows Application Event Log.

Table 10-2 lists the events for which messages are generated at each logging level.

Table 10-2  Events by logging level

<table>
<thead>
<tr>
<th>Logging level</th>
<th>Events logged</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>None</td>
</tr>
</tbody>
</table>
Table 10-2: Events by logging level (continued)

<table>
<thead>
<tr>
<th>Logging level</th>
<th>Events logged</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Error</strong></td>
<td>The following events are logged:</td>
</tr>
<tr>
<td></td>
<td>■ All of the events that are logged at the Audit logging level</td>
</tr>
<tr>
<td></td>
<td>■ Definitions corrupted</td>
</tr>
<tr>
<td></td>
<td>■ Definitions update failure</td>
</tr>
<tr>
<td></td>
<td>■ Licensing error</td>
</tr>
<tr>
<td></td>
<td>■ RPC Client Retry Error</td>
</tr>
<tr>
<td></td>
<td>■ Scan error</td>
</tr>
<tr>
<td></td>
<td>■ Critical error</td>
</tr>
<tr>
<td></td>
<td>■ Crash error</td>
</tr>
</tbody>
</table>
|               | ■ Logging error (SMTP/SNMP/RPC user notification)  
Entries for this event are only logged to the local logs. |
|               | ■ RPC client disconnected error |
|               | ■ Rapid Release antivirus definitions update failure |
|               | ■ File name exceeded |
|               | ■ Group resolve failed (Active Directory-based authentication mode) |
|               | ■ Authentication error (Active Directory-based authentication mode) |
|               | ■ There was an error running content update (Insight) |
|               | ■ Symantec Protection Engine has failed to connect to RPC client |
|               | ■ The Symantec Protection Engine has encountered an error (APK Reputation) |
| **Outbreak**  | The following events are logged: |
|               | ■ All of the events that are logged at the Error logging level |
|               | ■ File attribute outbreak alert |
|               | ■ URL block outbreak alert |
|               | ■ Malformed container outbreak alert |
|               | ■ Mail policy outbreak alert |
|               | ■ Nonviral outbreak alert |
|               | ■ Viral outbreak alert |
|               | ■ Container limit outbreak alert |
|               | ■ A threat outbreak has been detected (Insight) |
Table 10-2  Events by logging level (continued)

<table>
<thead>
<tr>
<th>Logging level</th>
<th>Events logged</th>
</tr>
</thead>
<tbody>
<tr>
<td>Warning</td>
<td>The following events are logged:</td>
</tr>
<tr>
<td></td>
<td>■ All of the events that are logged at the Outbreak logging level</td>
</tr>
<tr>
<td></td>
<td>■ Definitions rollback failed</td>
</tr>
<tr>
<td></td>
<td>■ Infection found</td>
</tr>
<tr>
<td></td>
<td>■ Spyware Risk</td>
</tr>
<tr>
<td></td>
<td>■ Adware Risk</td>
</tr>
<tr>
<td></td>
<td>■ Other Security Risk</td>
</tr>
<tr>
<td></td>
<td>■ Container violation found</td>
</tr>
<tr>
<td></td>
<td>■ File attribute violation found</td>
</tr>
<tr>
<td></td>
<td>■ Definitions rollback</td>
</tr>
<tr>
<td></td>
<td>■ Mail policy violation found</td>
</tr>
<tr>
<td></td>
<td>■ Licensing warning</td>
</tr>
<tr>
<td></td>
<td>■ URL block</td>
</tr>
<tr>
<td></td>
<td>■ File Access Allowed</td>
</tr>
<tr>
<td></td>
<td>■ Symantec Protection Engine has not received configured number of requests</td>
</tr>
<tr>
<td></td>
<td>■ Scanning feature hung or protection engine is overloaded</td>
</tr>
<tr>
<td></td>
<td>■ Scan request rejected</td>
</tr>
<tr>
<td></td>
<td>■ Failed to set Rapid Release parameters</td>
</tr>
<tr>
<td></td>
<td>■ Failed to create self scan test file</td>
</tr>
<tr>
<td></td>
<td>■ User authorization failed (Active Directory-based authentication mode)</td>
</tr>
<tr>
<td></td>
<td>■ Account locked out (Active Directory-based authentication mode)</td>
</tr>
<tr>
<td></td>
<td>■ User login failed</td>
</tr>
<tr>
<td></td>
<td>■ An infection has been found (Insight)</td>
</tr>
<tr>
<td></td>
<td>■ A security risk has been found (Insight)</td>
</tr>
<tr>
<td></td>
<td>■ Bad ICAP request</td>
</tr>
<tr>
<td></td>
<td>■ AV Connector has been disabled</td>
</tr>
<tr>
<td></td>
<td>■ A VServer has been disconnected from AV Connector</td>
</tr>
<tr>
<td></td>
<td>■ Symantec Protection Engine has failed to extract the file</td>
</tr>
<tr>
<td></td>
<td>■ An APK Reputation violation has been found (APK Reputation)</td>
</tr>
</tbody>
</table>
Table 10-2 Events by logging level (continued)

<table>
<thead>
<tr>
<th>Logging level</th>
<th>Events logged</th>
</tr>
</thead>
</table>
| Information   | The following events are logged:  
|               | - All of the events that are logged at the Warning logging level  
|               | - Version information  
|               | - URL audit detection  
|               | - Definitions update  
|               | - LiveUpdate up-to-date  
|               | - LiveUpdate succeeded  
|               | - User logged in  
|               | - Symantec Protection Engine has not scanned the file  
|               | - Symantec Protection Engine has updated one of its content (Insight)  
|               | - The AV Connector version and status information is provided  
|               | - The Symantec Protection Engine could not load all APK cache entries in memory from disk |
| Verbose       | The following events are logged:  
|               | - All of the events that are logged at the Information logging level  
|               | - Outbreak alerts for the configured events  
|               | - All of the events that are logged at the Warning logging level  
|               | - All of the events that are logged at the Information logging level  
|               | - Files scanned  
|               | - URLs scanned  
|               | **Note:** The Verbose logging level should only be selected for debugging purposes. Performance is significantly degraded if you activate this logging level for general logging. |

See “Logging destinations” on page 200.

Specifying the log bind address

You can set a log bind address for each Symantec Protection Engine so that you can more easily identify the originating protection engine. When you use this feature, the log bind address of the originating Symantec Protection Engine is included in all alert messages.

For example, setting the log bind address is helpful if you have multiple Symantec Protection Engines that listen on the loopback interface (127.0.0.1). The IP address on which Symantec Protection Engine listens is used in SNMP and SMTP alert messages to identify the originating Symantec Protection Engine. Therefore, it is not possible to determine which Symantec Protection Engine originated the message.
when more than one uses the loopback interface. You can set a unique log bind
address for each Symantec Protection Engine to provide a method for identifying
each Symantec Protection Engine.

If your client uses ICAP and you do not specify a log bind address, Symantec
Protection Engine selects one for you. Symantec Protection Engine determines the
log bind address based on the scanning bind addresses that you enable on the
Configuration > Protocol page.

Symantec Protection Engine determines the log bind address based on the following
conditions:

<table>
<thead>
<tr>
<th>No bind address is selected in the ICAP Configuration Bind address table.</th>
<th>The logging bind address is the first bind address in the ICAP Configuration Bind address table on the Configuration &gt; Protocol page.</th>
</tr>
</thead>
<tbody>
<tr>
<td>If the first bind address is the localhost, then the Logging IP address is the second bind address in the list.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>One or more bind addresses are selected in the ICAP Configuration Bind address table.</th>
<th>The logging bind address is the first non-local host IP address from the selected bind addresses in the ICAP Configuration Bind address table on the Configuration &gt; Protocol page.</th>
</tr>
</thead>
</table>

See “Specifying the log bind address in the Core server only mode” on page 305.
See “Configuring ICAP options” on page 98.

To specify the log bind address

1. In the console on the primary navigation bar, click **Monitors**.
2. In the sidebar under **Views**, click **Logging**.
3. In the content area under **Logging Properties**, in the **Log bind address** box, type an IP address to identify the computer on which Symantec Protection Engine is running.
4. On the toolbar, select one of the following options:
   
   **Save** Saves your changes.
   
   Use this option to continue making changes in the console until you are ready to apply them.

   **Apply** Applies your changes.
   
   Your changes are not implemented until you apply them.
About configuring local logging

You can change the types of events that are logged to the local logs.
You can also perform any of the following tasks:

■ Change the local logging level.
  See “Specifying the local logging level” on page 207.

■ Change the directory where log files are located.
  See “Changing the directory where log files are located” on page 208.
  See “Maintaining log files on a shared resource in Windows” on page 209.

■ Change the length of time that the log files are maintained.
  See “Changing the length of time that log files are maintained” on page 210.

■ Enable statistics reporting.
  See “Enabling statistics reporting in Symantec Protection Engine” on page 211.

■ Enable resource consumption logging.
  See “Enabling resource consumption logging in Symantec Protection Engine” on page 152.

Specifying the local logging level

Symantec Protection Engine sends logging events to the local logs by default. You can change the types of events that are sent to the local logs. The default logging level for the local logs is Warning.

See “Specifying the local logging level in the Core server only mode” on page 306.

To specify the local logging level

1  In the console on the primary navigation bar, click Monitors.

2  In the sidebar under Views, click Logging.
3 In the content area under **Local Logging**, in the **Local logging level** list, select the appropriate local logging level.

The default logging level is Warnings. Select Verbose only if you have been instructed to do so by Symantec Technical Support to troubleshoot issues.

4 On the toolbar, select one of the following options:

- **Save** Saves your changes.
  - Use this option to continue making changes in the console until you are ready to apply them.

- **Apply** Applies your changes.
  - Your changes are not implemented until you apply them.

See “Changing the directory where log files are located” on page 208.

### Changing the directory where log files are located

You can change the location of the local log file and the statistics log files. You cannot change the file names. The default location for the log files for Linux is `opt/SYMC Scan/log`. The default location for Windows platform is `C:\Program Files\Symantec\Scan Engine\log\`.

Symantec Protection Engine creates a new local log file for each day. The file names have the following format: `SSEyyyyymmdd.log`, where `yyyy` is the year, `mm` is the month, and `dd` is the day.

The disk space that is required for the log files varies, depending upon your scan volume, associated activity, and how long you retain the log files. The specified location must be large enough to accommodate these files. If you change the log file location, old log files remain in the former directory and are not removed during uninstallation. Old logs must be removed manually.

See “Changing the directory where log files are located in the Core server only mode” on page 307.

See “Changing the length of time that log files are maintained” on page 210.

To change the directory where log files are located

1 In the console on the primary navigation bar, click **Monitors**.

2 In the sidebar under **Views**, click **Logging**.
3 In the content area under **Local Logging**, in the **Log files directory** box, type the path to the new location for the log files.

The file directory that you specify must already exist. Symantec Protection Engine validates the existence of the directory when you save or apply your changes.

4 On the toolbar, select one of the following options:

- **Save**
  - Saves your changes.
  - Use this option to continue making changes in the console until you are ready to apply them.

- **Apply**
  - Applies your changes.
  - Your changes are not implemented until you apply them.

### Maintaining log files on a shared resource in Windows

You can store the Symantec Protection Engine log files on a shared resource. Make sure that the shared resource has adequate disk space. To optimize security, you should restrict full access rights on the shared resource to the administrator user of the host on which Symantec Protection Engine is installed.

**Note:** To enhance Symantec Protection Engine performance, maintain the log files locally instead of writing log data to a remote, shared resource.

Before you perform the following procedure, ensure that you are an administrator of the host on which Symantec Protection Engine is installed. Also ensure that you have full permissions on the shared resource.

See “Maintaining log files on a shared resource in Windows in the Core server only mode” on page 308.

**To maintain log files on a shared storage in Windows**

1 Map or mount the shared resource from the host on which Symantec Protection Engine is installed.

   For more information about how to map or mount a shared resource, see the documentation for your operating system.

2 Stop the Symantec Protection Engine service.

3 Change the account of the Symantec Protection Engine service to the Administrator.
4 Restart the Symantec Protection Engine service.

5 In the console on the primary navigation bar, click Monitors, and then click Logging.

6 Under Local Logging, in the Log files directory box, type the fully qualified path to the shared directory where you want the log file to reside.

   For example, <drive>:\logfiles

7 On the toolbar, select one of the following options:

   **Save** Saves your changes.
   
   Use this option to continue making changes in the console until you are ready to apply them.

   **Apply** Applies your changes.
   
   Your changes are not implemented until you apply them.

See “Verifying, stopping, and restarting the Symantec Protection Engine service on Windows” on page 62.

### Changing the length of time that log files are maintained

Symantec Protection Engine creates a new log file for each day. You can specify the number of log files that Symantec Protection Engine retains to keep the log directory at a manageable size. Thus, when the maximum number of log files is reached, the oldest log file is removed on a daily basis. In its default configuration, this setting is enabled and the default value is 0. That means all the log files are retained.

See “Exporting local log data to a file” on page 220.

**To change the length of time that log files are maintained**

1 In the console on the primary navigation bar, click Monitors.

2 In the sidebar under Views, click Logging.
3 In the content area under **Local Logging**, in the **Number of log files to retain (one per day)** box, type the number of individual log files to retain.

The default setting is enabled (0) so that all the log files are retained.

4 On the toolbar, select one of the following options:

- **Save** Saves your changes.
  
  Use this option to continue making changes in the console until you are ready to apply them.

- **Apply** Applies your changes.
  
  Your changes are not implemented until you apply them.

### Enabling statistics reporting in Symantec Protection Engine

You can configure Symantec Protection Engine to maintain and report cumulative scan data. You must enable logging to the statistics logs so that you can view statistics reports. You can select a date range and time range for the report and view the scanning statistics for that range.

See “**Viewing statistics log data**” on page 221.

Symantec Protection Engine creates a new statistics log file for each day. The file name has the following format: SSEyyyymmdd.dat, where yyyy is the year, mm is the month, and dd is the day.

The statistics log files are stored in the same location as the log files. The default location for the log files for Linux is /opt/SYMCScan/log. The default location for Windows platform is C:\Program Files\Symantec\ScanEngine\log\.

See “**Enabling statistics reporting in the Core server only mode**” on page 310.

See “**Changing the length of time that log files are maintained**” on page 210.

**To enable statistics reporting**

1 In the console on the primary navigation bar, click **Monitors**.

2 In the sidebar under **Views**, click **Logging**.
In the content area under **Local Logging**, check **Enable statistics reporting**. Statistics reporting is enabled by default.

On the toolbar, select one of the following options:

**Save**
- Saves your changes.
- Use this option to continue making changes in the console until you are ready to apply them.

**Apply**
- Applies your changes.
- Your changes are not implemented until you apply them.

See “About configuring local logging” on page 207.

---

**Configuring logging to the Windows Application Event Log**

If you are running Symantec Protection Engine on Windows, you can configure Symantec Protection Engine to log events to the Windows Application Event Log. You can also select the types of events that are logged. The default logging level is None (deactivated).

See “Configuring logging to the Windows Application Event Log in the Core server only mode” on page 311.

**To configure logging to the Windows Application Event Log**

1. In the console on the primary navigation bar, click **Monitors**.
2. In the sidebar under **Views**, click **Logging**.
3. In the content area under **Windows Logging**, in the **Windows logging level** list, select the appropriate logging level.
   - The default logging level for the Windows Application Event Log is None.
4. On the toolbar, select one of the following options:
   - **Save** saves your changes.
     - Use this option to continue making changes in the console until you are ready to apply them.
   - **Apply** applies your changes.
     - Your changes are not implemented until you apply them.
See “Logging levels and events” on page 202.

### Configuring logging to the Linux Syslog

If you are running Symantec Protection Engine on Linux, you can configure Symantec Protection Engine to log events to the Linux Syslog. You can also select the types of events that are logged. The default logging level is None (deactivated). Logs are saved at `/var/log/messages` location.

You must be running Symantec Protection Engine on Linux to use this feature.

**To configure logging to the Linux Syslog**

1. In the console on the primary navigation bar, click **Monitors**.
2. In the sidebar under **Views**, click **Logging**.
3. In the content area under **Linux Syslog Logging**, in the **Linux logging level** list, select the appropriate logging level.

   The default logging level for the Linux Syslog is **None**.

4. On the toolbar, select one of the following options:

   - **Save**: Saves your changes.
     
     Use this option to continue making changes in the console until you are ready to apply them.

   - **Apply**: Applies your changes.
     
     Your changes are not implemented until you apply them.

See “Configuring logging to the Linux Syslog in the Core server only mode” on page 312.

### About configuring alerts

In addition to the local log, you can send alerts using Simple Network Management Protocol (SNMP) and Simple Mail Transfer Protocol (SMTP). You can select a notification level to control the amount and the type of alerts that are sent.

See “Activating SMTP alerts” on page 214.

See “Activating SNMP alerts” on page 215.

If you activate SNMP or SMTP alerts and are running multiple Symantec Protection Engines, set a log bind address for each one. Separate log bind addresses let you
identify the originating Symantec Protection Engine for each SNMP and SMTP alert message.

See “Specifying the log bind address” on page 205.

You also can activate outbreak alerts. Symantec Protection Engine can issue alerts when a specified number of the same type of threat or violation occurs in a given time interval. Outbreak alerts provide an early warning of a potential outbreak so that you can take the necessary precautions to protect your network.

See “Configuring outbreak alerts” on page 216.

### Activating SMTP alerts

When you activate SMTP alerts, you must identify a primary SMTP server for forwarding alert messages. You must also specify the email addresses of the recipients and the local domain for Symantec Protection Engine. You can specify a second SMTP server if one is available.

You must select the types of events for which SMTP alert messages are generated.

See “Activating SMTP alerts in the Core server only mode” on page 312.

See “Logging levels and events” on page 202.

**To activate SMTP alerts**

1. In the console on the primary navigation bar, click **Monitors**.
2. In the sidebar under **Views**, click **Alerting**.
3. In the content area under **SMTP Notifications**, in the **SMTP notification level** list, select the SMTP notification level.

   SMTP alerts are not activated by default. The SMTP notification level is set to None. The Verbose notification level is not available for SMTP alerting.

4. In the **Primary server address** box, type the IP address or host name of the primary SMTP server that forwards the alert messages.
5. In the **Secondary server address** box, type the IP address or host name of a secondary SMTP server (if one is available) that forwards the alert messages if communication with the primary SMTP server fails.
6. In the **SMTP domain** box, type the local domain for Symantec Protection Engine.

   The domain name is added to the From box for SMTP messages. SMTP alert messages that Symantec Protection Engine generates originate from SymantecProtectionEngine@<domainname>, where <domainname> is the domain name that you specify in the SMTP domain box.
In the Email recipients box, type the email addresses of the recipients of the SMTP alert messages.
Type one email address per line.

On the toolbar, select one of the following options:

Save
Saves your changes.
Use this option to continue making changes in the console until you are ready to apply them.

Apply
Applies your changes.
Your changes are not implemented until you apply them.

See “About configuring alerts” on page 213.

Activating SNMP alerts

To activate SNMP alerts, you must provide the SNMP community string and an IP address for a primary SNMP console for receiving the alert messages. You can specify a second SNMP console if one is available. A secondary SNMP console is optional. Alert messages are sent to the primary SNMP console and secondary SNMP console in all instances. You can also configure ports for the primary server and secondary server.

The Management Information Base file (symantecprotectionengine.mib) is located in the Tools\MIB folder in the Symantec_Protection_Engine_Tools_7.9.0.XX_IN.zip file. You can use the symantecprotectionengine.mib file to configure the SNMP alerts.

You must select the types of events for which SNMP alert messages are generated.
See “Activating SNMP alerts in the Core server only mode” on page 314.
See “Logging levels and events” on page 202.

To activate SNMP alerts

1. In the console on the primary navigation bar, click Monitors.
2. In the sidebar under Views, click Alerting.
3. In the content area under SNMP Notifications, in the SNMP notification level list, select the SNMP notification level.

SNMP alerts are not activated by default. The SNMP notification level is set to None. The Verbose notification level is not available for SNMP alerting.
4 In the **Primary server address** box, type the computer name or IP address of the primary SNMP console to receive the alert messages.

5 In the **Primary server port** box, type the port of the primary SNMP console to receive the alert messages.

   The default value is 162.

6 In the **Secondary server address** box, type the computer name or IP address of a secondary SNMP console to receive the alert messages, if one is available.

7 In the **Secondary server port** box, type the port of a secondary SNMP console to receive the alert messages, if one is available.

   The default value is 162.

8 In the **SNMP community** box, type the SNMP community string.

   The default setting is public.

9 On the toolbar, select one of the following options:

   **Save**  
   Saves your changes.

   Use this option to continue making changes in the console until you are ready to apply them.

   **Apply**  
   Applies your changes.

   Your changes are not implemented until you apply them.

See “**About configuring alerts**” on page 213.

### Configuring outbreak alerts

Symantec Protection Engine can issue alerts when a specified number of the same type of threat or policy violation occurs in a given time interval. You can use outbreak alerts as an early warning for potential outbreaks. Alerts of outbreaks can help you take the necessary precautions to protect your network.

You can select the types of events for which you want to receive alerts. For each event type, you can configure the threshold number of occurrences and the time interval. If the number of occurrences meets or exceeds the configured threshold for the selected interval, Symantec Protection Engine generates an alert.

See “**Configuring outbreak alerts in the Core server only mode**” on page 316.

**Table 10-3** lists the outbreak alert events that you can configure.
Table 10-3  Outbreak alert events

<table>
<thead>
<tr>
<th>Event</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any viral threat</td>
<td>A viral threat was detected</td>
</tr>
<tr>
<td>Same viral threat</td>
<td>One or more incidence of the same type of viral threat was detected</td>
</tr>
<tr>
<td>Mail policy violations</td>
<td>A mail policy violation occurred</td>
</tr>
<tr>
<td>Blocked URLs</td>
<td>A URL was blocked due to a URL filtering violation</td>
</tr>
<tr>
<td>Container limit</td>
<td>A maximum file extraction time/size/depth was met or exceeded</td>
</tr>
<tr>
<td>Malformed containers</td>
<td>A malformed container was detected and blocked</td>
</tr>
<tr>
<td>File attribute</td>
<td>Any file attribute violation was detected</td>
</tr>
<tr>
<td>Any nonviral threats</td>
<td>A nonviral threat was detected</td>
</tr>
<tr>
<td>Same nonviral threat</td>
<td>One or more incidence of the same type of nonviral threat was detected</td>
</tr>
<tr>
<td>High risk rating threats</td>
<td>A high risk rating threat was detected</td>
</tr>
<tr>
<td>Medium risk rating threats</td>
<td>A medium risk rating threat was detected</td>
</tr>
<tr>
<td>Insight threats</td>
<td>A threat was detected by Insight</td>
</tr>
</tbody>
</table>

To configure outbreak alerts

1. In the console on the primary navigation bar, click Monitors.
2. In the sidebar under Views, click Outbreak.
3. In the content area under Outbreak Management, check the events for which you want to receive alerts.
   You must select Outbreak alerting (or a higher logging level that includes outbreak alerting) for at least one logging destination to generate an outbreak alert.
4. For each selected event type, do the following in the order given:
   - Under Occurrences, type the occurrence threshold.
     The default value is 2. You can use any value from 2 to 100000.
Under **Time Interval**, type the number of minutes within which the threshold number of events must occur to generate an outbreak alert. The default value is 1. You can use any range from 1 to 100000.

5 On the toolbar, select one of the following options:

- **Save** Saves your changes.
  
  Use this option to continue making changes in the console until you are ready to apply them.

- **Apply** Applies your changes.
  
  Your changes are not implemented until you apply them.

See “About configuring alerts” on page 213.

See “Logging levels and events” on page 202.

**About reports**

You can use the Symantec Protection Engine reporting functionality to manage your local log file data. The log data that is stored in the log files depends on the logging level that you select for local logging. Local logging is activated by default at the Warning level. If you select a type of log entry for a report that is not logged at the configured logging level, no data is available.

When working in the Core server with user interface mode, you can manage reports through the Symantec Protection Engine console by doing any of the following actions:

- Generate a report of log data from the local logs.
  
  The local log files cannot be read directly. You must use the reporting function to view the local logs. Local logging is the default logging destination.
  
  See “Viewing the local log data” on page 219.

- Export selected local log data in a comma-separated value (.csv) format.
  
  See “Exporting local log data to a file” on page 220.

- Generate a report of statistics information that is contained in the statistics logs.
  
  The statistics log files are in .csv format and can be read or imported into a spreadsheet program. You must use the reporting function to view the statistics logs.
  
  See “Viewing statistics log data” on page 221.

- View summary report on Symantec Protection Engine home page.
When working in the Core server only mode, you can manage reports, using the LogConverter.exe utility provided in the installation directory, by doing any of the following actions:

- Generate a report of log data from the local logs in plain text format.
- Export local log data in a comma-separated value (.csv) format.
- Export local log data in an html format.

See “About the Core server only mode” on page 249.

Viewing the local log data

You can use the reporting feature to view the log data from the local logs. The local log files cannot be read directly. The reporting feature formats the local logs in an HTML table that displays in the browser window. You can choose a date range and time range for which you want to view log data. You can also select one or more types of log entries that you want to view.

Local logging is the default logging destination. Local logging is activated by default at the Warning level. The log data that is stored in the log files depends on the logging level that you select for local logging. If you select a type of log entry for a report that is not logged at the configured logging level, no data is available.

See “Logging levels and events” on page 202.

**Note:** To view the HTML report, you must disable any pop-up blockers that are running on your computer.

To view the local log data

1. In the console on the primary navigation bar, click **Reports**.
2. In the sidebar under **Views**, click **Detailed**.
3. In the content area under **Log View Page**, in the **Date range from** boxes, type the start date and the end date for the range you want to report.

   Use the following date format:

   MM/DD/YY

   For example, 02/25/08 is February 25, 2008.
4 In the **Time range from** boxes, type the daily start times and the end times for the time range that you want to report.

Use the following time format:

HH:MM:SS

Use a 24-hour time format. For example, 23:30:00 is 11:30 P.M.

5 Check any activities for which you want to view the log data.

Check all of the options that apply.

Press **Ctrl+A** to select all items in every category. Press **Ctrl+Z** to unselect all items in every category.

6 In the sidebar under **Tasks**, click **Generate Report**.

See “**About reports**” on page 218.

---

### Exporting local log data to a file

You can export the log data to a file in a comma-separated value (.csv) format. You can choose a date range and time range for which you want to export data. You can also select one or more types of log entries that you want to export.

---

**Note:** If you try to download large log files during periods of peak usage, the performance of Symantec Protection Engine might be affected.

---

To export local log data to a file

1 In the console on the primary navigation bar, click **Reports**.

2 In the sidebar under **Views**, click **Detailed**.

3 In the content area under **Log View Page**, in the **Date range from** boxes, type the start date and end dates for the date range that you want.

Use the following date format:

MM/DD/YY

For example, 02/25/08 is February 25, 2008.

4 In the **Time range from** boxes, type the daily start times and the end times for the time range that you want.

Use the following time format:

HH:MM:SS

Use a 24-hour time format. For example, 23:30:00 is 11:30 P.M.
5. Check any activities for which you want to export the log data. Check all of the options that apply. Press Ctrl+A to select all items in every category. Press Ctrl+Z to unselect all items in every category.

6. In the sidebar under Tasks, click Export (CSV).

7. In the Save logs dialog box, in the Save in list, select the file location where you want to save the report.

8. In the File name box, type the file name, and then click Save.

See “About reports” on page 218.

Viewing statistics log data

You can use the reporting feature to view the log data from the statistics logs. You can choose a date range and time range for which you want to view the statistics data. You can also select one or more types of statistics that you want to view.

Statistic logs are used to report the following cumulative scan data:

- Total number of files that are scanned, repaired, and quarantined and also the total megabytes scanned
- Number of files rated as high, medium or low risk.
- Number of infected files and the number of infected files that are repaired.
- Number of viruses found and security risks detected by Insight
- Types of violations that Symantec Protection Engine found by violation type
- Number of malformed and encrypted containers
- Total number of scanned and blocked URLs and the number of URL audits

Note: You must enable logging to the statistics logs. After you enable logging to the statistics logs, you can use the statistics reporting feature to view the statistics.

You can obtain summary data from the local logs for a given period of time. For the reported period, you can review the total number of risks that were found and the total number of files that were repaired.

The default logging destination for Symantec Protection Engine is the local logs. The default location for the local logs on Linux is /opt/SYMCScan/log. The default location for Windows platform is C:\Program Files\Symantec\Scan Engine\log\. You can change the location of the logs.
See “Changing the directory where log files are located” on page 208.

The statistics do not represent a literal physical file count of the total number of files that have been scanned. This total includes not only the number of files but also the additional objects within the container files that were scanned. Some containers (such as MIME-encoded messages and Microsoft Office documents) have additional embedded objects. These embedded objects might not be files, but they might be scanned depending on the files that you have selected for scanning. The total does not include any objects within the container files that were not scanned because their extensions did not match those configured for scanning.

To view statistics log data

1. In the console on the primary navigation bar, click **Reports**.
2. In the sidebar under **Views**, click **Statistics**.
3. In the content area under **Statistics View**, in the **Date range from** boxes, type the start date and end date for the range you want to report.
   Use the following date format:
   MM/DD/YY
   For example, 02/25/08 is February 25, 2008.
4. In the **Time range from** boxes, type the daily start and end times for which you want to report.
   Use the following time format:
   HH:MM:SS
   Use a 24-hour time format. For example, 23:30:00 is 11:30 P.M.
5. In the sidebar under **Tasks**, click **Generate Report**.

See “About reports” on page 218.

About summary report on Symantec Protection Engine home page

The home page of Symantec Protection Engine displays summary of all scanning activities.

Symantec Protection Engine displays the following summary:
### Table 10-4  Symantec Protection Engine summary

<table>
<thead>
<tr>
<th>Category</th>
<th>Activity</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Overall Viral Statistics</strong></td>
<td>■ Viruses found</td>
</tr>
<tr>
<td></td>
<td>* <strong>Note:</strong> Includes the count from Insight detected viruses.</td>
</tr>
<tr>
<td></td>
<td>■ Viruses repaired</td>
</tr>
<tr>
<td><strong>Generic Status</strong></td>
<td>■ Total requests</td>
</tr>
<tr>
<td></td>
<td>■ URLs scanned</td>
</tr>
<tr>
<td></td>
<td>■ Files scanned</td>
</tr>
<tr>
<td></td>
<td>■ Total files scanned</td>
</tr>
<tr>
<td></td>
<td>■ Data scanned</td>
</tr>
<tr>
<td></td>
<td>■ Total data scanned</td>
</tr>
<tr>
<td><strong>Overall Non Viral Statistics</strong></td>
<td><strong>Security Risks</strong></td>
</tr>
<tr>
<td></td>
<td>* <strong>Note:</strong> Includes the count from Insight detected security risks.</td>
</tr>
<tr>
<td><strong>Quarantine</strong></td>
<td>Files quarantined</td>
</tr>
<tr>
<td><strong>Insight Statistics</strong></td>
<td>■ Viruses found</td>
</tr>
<tr>
<td></td>
<td>■ Security risks</td>
</tr>
<tr>
<td>* <strong>Note:</strong> Viruses found and Security risks under Overall Viral statistics and Overall Non Viral Statistics, include the count from Insight detected viruses and Insight detected security risks respectively.</td>
<td></td>
</tr>
<tr>
<td><strong>Filtering</strong></td>
<td>■ URL Filtering Blocks</td>
</tr>
<tr>
<td></td>
<td>■ URL Reputation Blocks</td>
</tr>
</tbody>
</table>

From version 7.0, Symantec Protection Engine is capable of calculating and retaining cumulative scan data since installation in addition to retaining data since last restart. You can configure the following on the Symantec Protection Engine home page:

- Display summary since installation.
- Display summary since last restart.
- Auto-refresh the home page every one minute.

Symantec Protection Engine home page also shows a graphical representation of scanning activities and threat risk ratings for the selected time frame.
See “Viewing summary report on Symantec Protection Engine home page” on page 224.

See “Auto-refreshing Symantec Protection Engine home page” on page 225.

Viewing summary report on Symantec Protection Engine home page

The Symantec Protection Engine home page displays summary of all scanning activities. You can configure Symantec Protection Engine to display a summary of scanning activities since installation or last restart. Symantec Protection Engine also shows a graphical representation of scanning activities for the selected time frame.

To view summary report on Symantec Protection Engine home page

1. In the console on the primary navigation bar, click Home.
2. In the content area, in the Report Statistics Since drop-down list select any one of the following:

   - Installation: Displays a summary report of scanning activities since installation.
   - Last Restart: Displays a summary report of scanning activities since last restart.
     By default, Symantec Protection Engine displays scanning activities since last restart.

3. On the toolbar, select one of the following options:

   - Save: Saves your changes.
     Use this option to continue making changes in the console until you are ready to apply them.
   - Apply: Applies your changes.
     Your changes are not implemented until you apply them.

See “About summary report on Symantec Protection Engine home page” on page 222.

See “Auto-refreshing Symantec Protection Engine home page” on page 225.
Auto-refreshing Symantec Protection Engine home page

The Symantec Protection Engine home page displays the summary of scanning activities. You can configure Symantec Protection Engine to auto-refresh the home page every one minute to display the latest cumulative scan data.

To auto-refresh Symantec Protection Engine home page

1. In the console on the primary navigation bar, click Home.
2. In the content area, select the Auto Refresh box.
   Symantec Protection Engine automatically refreshes the home page every one minute.
3. On the toolbar, select one of the following options:
   - Save: Saves your changes. Use this option to continue making changes in the console until you are ready to apply them.
   - Apply: Applies your changes. Your changes are not implemented until you apply them.

See “About summary report on Symantec Protection Engine home page” on page 222.

See “Viewing summary report on Symantec Protection Engine home page” on page 224.
Keeping your product up to date

This chapter includes the following topics:

- About content updates
- About LiveUpdate
- About Intelligent Update
- About Rapid Release
- Rolling back definitions

About content updates

The content updates ensure that your Symantec Protection Engine server is up-to-date with the most current Antivirus and URL definitions. You can update Symantec Protection Engine with the latest definitions without any interruption in scanning.

See “About licensing” on page 88.

About definition updates

Symantec provides updates for the following types of definitions:

**Antivirus**

Definition files contain the necessary information to detect and eliminate risks, such as viruses and adware. Symantec supplies updated definition files every day and whenever a new risk is discovered.

You can update antivirus definitions using LiveUpdate, Rapid Release, or Intelligent Update.
Symantec periodically supplies updated URL definition files. If you subscribe to content updates, Symantec Protection Engine automatically downloads updated URL definitions through LiveUpdate. Symantec might create new URL categories to address emerging URLs as needed. If you subscribe to the content updates, any new categories are automatically downloaded with the regular updates to the existing categories.

You must update URL definitions using LiveUpdate.

Insight definition feeds are different in nature from that of AV definitions. Definition upgrade for Insight content are performed by APIs that add or remove the content information to the existing database and/or the reputation directory.

Rollback is not supported for any of the Insight specific content.

Symantec Protection Engine automatically uses the most current definition files for scanning. However, if a problem is discovered with the current definitions, you can revert (roll back) to the previous set of antivirus or URL definitions.

When you perform a content update, Symantec Protection Engine downloads and installs the most current definitions. If an error occurs, Symantec Protection Engine tries to roll back to the previous definitions. If the rollback is successful, Symantec Protection Engine continues scanning using the previous definitions. If the rollback is unsuccessful, scanning is disabled. You must have a valid license to update definitions.

See “Rolling back definitions” on page 245.

See “About licensing” on page 88.

About updating your protection
You can use several methods to update protection from risks and HTTP content filtering violations with Symantec Protection Engine.

Table 11-1 lists the methods that you can use to obtain updated definitions from Symantec.
### Table 11-1: Methods to obtain updated definitions from Symantec

<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
<th>How often Symantec provides updated definitions</th>
</tr>
</thead>
<tbody>
<tr>
<td>LiveUpdate</td>
<td>Use LiveUpdate to automatically update your protection. When LiveUpdate runs, it only downloads and installs the definitions that are more current than the definitions that are found on the Symantec Protection Engine server. You can configure LiveUpdate to run on a scheduled basis, or you can run it manually. See “About LiveUpdate” on page 229.</td>
<td>Daily, except in cases of outbreaks, when definitions are updated more often</td>
</tr>
<tr>
<td>Rapid Release</td>
<td>You can use Rapid Release when you need quick responses to emerging threats. Rapid Release definitions are most useful for a perimeter defense to mitigate quickly spreading threats. You can configure Rapid Release to run on a scheduled basis, or you can run it manually. See “About Rapid Release” on page 243.</td>
<td>Hourly</td>
</tr>
</tbody>
</table>
## Table 11-1 Methods to obtain updated definitions from Symantec *(continued)*

<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
<th>How often Symantec provides updated definitions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intelligent Update</td>
<td>Typically, Intelligent Update packages can be used in isolated networks where latest definitions are not available through LiveUpdate or Rapid Release. Based on your operating system on which Symantec Protection Engine is installed, you can download the appropriate Intelligent Update package from the Symantec FTP site. <strong>Note:</strong> Intelligent Update does not provide updated URL definitions. See “About Intelligent Update” on page 237.</td>
<td>Daily</td>
</tr>
</tbody>
</table>

You can use more than one method at a time to update your protection. You do not have to choose one or the other. For example, you can perform on-demand LiveUpdate definition updates and schedule Rapid Release definition updates to occur simultaneously.

You must have a valid content license to install definition files. A content license is a grant by Symantec Corporation for you to update Symantec corporate software with the latest associated content, such as new definitions. When you do not have a content license or your license expires, your product does not receive the most current definitions. Outdated definitions can leave your servers vulnerable to risks.

See “About licensing” on page 88.

### About LiveUpdate

When you install or upgrade Symantec Protection Engine, LiveUpdate is enabled by default to run every two hours. You can modify this schedule, or you can run LiveUpdate manually. You can also use the XML modifier command-line tool to configure the number of times Symantec Protection Engine tries to perform a LiveUpdate.

The Symantec Protection Engine LiveUpdate configuration file contains the configuration options for LiveUpdate. The LiveUpdate configuration file is stored the following locations by default:
When Symantec Protection Engine performs a LiveUpdate, the definitions that are downloaded are automatically selected as the active definitions. However, you can revert to the previous versions of the antivirus or URL definitions. The definition set that you choose remains active until the next LiveUpdate or Rapid Release update occurs, which then becomes the active definition set.

To edit the LiveUpdate server details, See “Configure the LiveUpdate server details” on page 373.

See “Configure the number of LiveUpdate retries” on page 372.

See “Configuring LiveUpdate to occur automatically” on page 230.

See “Performing LiveUpdate on demand” on page 231.

See “Rolling back definitions” on page 245.

### Configuring LiveUpdate to occur automatically

You can schedule LiveUpdate to occur automatically at a specified time interval to ensure that Symantec Protection Engine always has the most current definitions. When you install a valid antivirus content license or URL content license, Symantec Protection Engine automatically tries to perform a LiveUpdate. By default, Symantec Protection Engine is configured to perform a LiveUpdate every two hours.

When LiveUpdate is scheduled, it runs at the specified time interval that is relative to the LiveUpdate base time. The default LiveUpdate base time is the time that Symantec Protection Engine was installed. You can change the LiveUpdate base time by editing the configuration file. If you change the scheduled LiveUpdate interval, the interval adjusts based on the LiveUpdate base time.

See “Configuring LiveUpdate to occur automatically in the Core server only mode” on page 319.

See “Change the LiveUpdate base time” on page 373.

To configure LiveUpdate to occur automatically

1. In the console on the primary navigation bar, click **System**.
2. In the sidebar under **Views**, click **LiveUpdate Content**.
3. In the content area under **LiveUpdate Content**, check **Enable scheduled LiveUpdate**.

   The default setting is enabled.
In the **LiveUpdate interval** drop-down list, select the interval. You can choose from 2, 4, 8, 10, 12, or 24-hour intervals. The default setting is 2 hours.

On the toolbar, select one of the following options:

- **Save**  
  Saves your changes.  
  Use this option to continue making changes in the console until you are ready to apply them.

- **Apply**  
  Applies your changes.  
  Your changes are not implemented until you apply them.

See “About LiveUpdate” on page 229.

### Performing LiveUpdate on demand

You can run LiveUpdate on demand to force an immediate update of definitions. If you have scheduled LiveUpdate, the next scheduled LiveUpdate try occurs at its scheduled time.

**To perform LiveUpdate on demand**

1. In the console on the primary navigation bar, click **System**.
2. In the sidebar under **Views**, click **LiveUpdate Content**.
3. Under **Definition Details**, select a definitions set that you want to update.
4. Under **Tasks**, click **LiveUpdate Content**.

See “About LiveUpdate” on page 229.

### About scheduling LiveUpdate using the command line

You can use the command line to schedule LiveUpdate. LiveUpdate ensures that Symantec Protection Engine always has the most current definitions. You must create an empty file within the directory in which Symantec Protection Engine is installed. The empty file name must be LUNowFlag. Symantec Protection Engine periodically checks for this file and performs a LiveUpdate when this file is present. Symantec Protection Engine automatically removes the file before the LiveUpdate command runs.

You can choose to create the LUNowFlag file periodically by using schedulers. If you use Windows, you can use the standard Windows scheduler. On Linux, you use the Unix cron scheduler.
About setting up your own LiveUpdate server

If you have multiple Symantec Protection Engines installed on your network, you might want to set up your own LiveUpdate server. With your own LiveUpdate server, you eliminate the need to have each Symantec Protection Engine on your network contact Symantec servers.

For more information, see the *LiveUpdate Administration Utility*, which is included in the *Symantec_Protection_Engine_Tools.zip* file.

See “Where to get more information” on page 28.

If you set up your own LiveUpdate server, you must edit the LiveUpdate configuration file (*liveupdate.xml*) for Symantec Protection Engine to point to the local LiveUpdate server. The *liveupdate.xml* file contains the configuration options for LiveUpdate. This file is stored at the following locations by default:

- **Linux**: `/opt/SYMCScan/bin/liveupdate.xml`
- **Windows**: `C:\Program Files\Symantec\Scan Engine\liveupdate.xml`

See “About editing the LiveUpdate XML file” on page 232.

See “About LiveUpdate” on page 229.

About editing the LiveUpdate XML file

You must configure LiveUpdate in the *liveupdate.xml* file so that Symantec Protection Engine always has the most current definition files.

See “About editing the Symantec Protection Engine configuration files” on page 365.

*Table 11-2* lists the default parameters that are added to the *liveupdate.xml* file.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol</td>
<td>Updated definition files are retrieved through HTTP. This information is required unless you use a host file. The default setting for the LiveUpdate transport protocol is HTTP. See “Configure the LiveUpdate server details” on page 373.</td>
</tr>
</tbody>
</table>
### Table 11-2  Default Parameters in liveupdate.xml file (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server name</td>
<td>Symantec Protection Engine contacts a specified server to check for and to retrieve updated definition files. You must supply the appropriate LiveUpdate server name. The default server is liveupdate.symantec.com. See “Configure the LiveUpdate server details” on page 373.</td>
</tr>
<tr>
<td>Port</td>
<td>You must specify the TCP/IP port the LiveUpdate server server is listening on. The default value is 80. See “Configure the LiveUpdate server details” on page 373.</td>
</tr>
<tr>
<td>Path</td>
<td>Specify the directory on the LiveUpdate server that contains the LiveUpdate packages. Note: This is an optional parameter. See “Configure the LiveUpdate server details” on page 373.</td>
</tr>
<tr>
<td>User name</td>
<td>Specify a user name to log on to the LiveUpdate server. Note: This is an optional parameter. See “Configure the LiveUpdate server details” on page 373.</td>
</tr>
<tr>
<td>Password</td>
<td>Specify a password to log on to the LiveUpdate server. Note: This is an optional parameter. See “Configure the LiveUpdate server details” on page 373.</td>
</tr>
</tbody>
</table>

### About LiveUpdate logging

Symantec Protection Engine downloads seven types of definitions to ensure that your network is up-to-date with the most current antivirus, URL, and Insight definitions.

*Table 11-3* lists the various LiveUpdate definitions and their description.
Table 11-3  LiveUpdate definitions

<table>
<thead>
<tr>
<th>Definition</th>
<th>Definition type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Antivirus</td>
<td>Antivirus</td>
<td>These definitions updates ensure that Symantec Protection Engine can detect potential threats and risks.</td>
</tr>
<tr>
<td>URL</td>
<td>Symantec URL</td>
<td>These definitions update the predefined URL categories.</td>
</tr>
<tr>
<td>CAIC URL</td>
<td></td>
<td>These definitions update the Child Abuse Image Content (CAIC) URL categories.</td>
</tr>
<tr>
<td>URL Reputation</td>
<td></td>
<td>These definitions update the IP, Domain/URL Reputation feeds.</td>
</tr>
<tr>
<td>Insight</td>
<td>Insight Settings</td>
<td>Insight Settings content is published very infrequently. The package size is generally around 6 to 9 KB.</td>
</tr>
<tr>
<td></td>
<td>Insight Cache Revocation Content</td>
<td>Insight Cache Revocation Content is usually published several times daily. The size is from 3 to 6 KB on an average.</td>
</tr>
<tr>
<td></td>
<td>Insight Sym VT Content</td>
<td>Insight Sym VT Content is published very infrequently (at most twice a year). The package size is of the order of 10s of KB.</td>
</tr>
</tbody>
</table>

**About types of logging**

The LiveUpdate definition status is logged in the following two types of logs:

- Basic LiveUpdate logs
  See “About basic LiveUpdate logs” on page 234.

- Detailed LiveUpdate logs
  See “About detailed LiveUpdate logs” on page 236.

**About basic LiveUpdate logs**

The basic logs provide a brief overview of the definition content status. These logs are enabled by default and their location is non configurable.

The following table lists the definition type and its default log location:
<table>
<thead>
<tr>
<th>Definition type</th>
<th>Log location</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Antivirus</strong></td>
<td>On UNIX platforms:</td>
</tr>
<tr>
<td></td>
<td>/opt/SYMCScan/bin/definitions/AntiVirus/Logs/lux.log</td>
</tr>
<tr>
<td></td>
<td>On Windows platforms:</td>
</tr>
<tr>
<td></td>
<td>C:\Program Files\Symantec\Scan Engine\Definitions\AntiVirus\Logs\lux.log</td>
</tr>
<tr>
<td><strong>Symantec URL</strong></td>
<td>On UNIX platforms:</td>
</tr>
<tr>
<td></td>
<td>/opt/SYMCScan/bin/definitions/URLListLookup/DefDownloads/SYM/Logs/lux.log</td>
</tr>
<tr>
<td></td>
<td>On Windows platforms:</td>
</tr>
<tr>
<td></td>
<td>C:\Program Files\Symantec\Scan Engine\Definitions\URLListLookup\DefDownloads\SYM\Logs\lux.log</td>
</tr>
<tr>
<td><strong>CAIC URL</strong></td>
<td>On UNIX platforms:</td>
</tr>
<tr>
<td></td>
<td>/opt/SYMCScan/bin/definitions/URLListLookup/DefDownloads/CAIC/Logs/lux.log</td>
</tr>
<tr>
<td></td>
<td>On Windows platforms:</td>
</tr>
<tr>
<td></td>
<td>C:\Program Files\Symantec\Scan Engine\Definitions\URLListLookup\DefDownloads\CAIC\Logs\lux.log</td>
</tr>
<tr>
<td><strong>URL Reputation</strong></td>
<td>On UNIX platforms:</td>
</tr>
<tr>
<td></td>
<td>/opt/SYMCScan/bin/definitions/URLRepLookup/URLReputationList/DefDownloads\URLREP\Logs\lux.log</td>
</tr>
<tr>
<td></td>
<td>On Windows platforms:</td>
</tr>
<tr>
<td></td>
<td>C:\Program Files\Symantec\Scan Engine\Definitions\URLRepLookup\URLReputationList\DefDownloads\URLREP\Logs\lux.log</td>
</tr>
<tr>
<td><strong>Insight Settings</strong></td>
<td>On UNIX platforms:</td>
</tr>
<tr>
<td></td>
<td>/opt/SYMCScan/bin/definitions/reputation/dwnlds/tiset/Logs/lux.log</td>
</tr>
<tr>
<td></td>
<td>On Windows platforms:</td>
</tr>
<tr>
<td></td>
<td>C:\Program Files\Symantec\Scan Engine\Definitions\reputation\dwnlds\tiset\Logs\lux.log</td>
</tr>
</tbody>
</table>
## About detailed LiveUpdate logs

The detailed logs provide a detailed definition content status. These logs are optional and disabled by default. Unlike the basic logs, the location of the detailed logs is configurable.

Enabling detailed logging of LiveUpdate can be done on Windows and Unix platforms. The configuration files required to enable detailed LiveUpdate logging are present in the `Symantec_Protection_Engine_Tools_7.9.0.XX_IN.zip` file.

### About enabling detailed LiveUpdate logging on Windows

On Windows platforms, you need to use a Windows software trace preprocessor (WPP) tracing mechanism to view the LiveUpdate log. For example, use TraceView that is a part of Windows Driver Kit (WDK).

When using the WPP tracing mechanism, the following files are required for enabling detailed logging of LiveUpdate on Windows platforms:

- `DefUtDCD.tmf`
- `defutils.ctl`
- `duluxcallback.tmf`
- `DuLuxTrace.ctl`
- `Lux.tmf`
- `LuxTrace.ctl`
About enabling detailed LiveUpdate logging on Unix

To enable detailed LiveUpdate logging on Unix

1. Copy the lux.logging.conf file from the
   Symantec_Protection_Engine_Tools_7.8.1.XX_IN.zip\Tools\LiveUpdate_Log_Config\folder into the \etc\symantec directory.

2. Copy the lux.logging.conf file from the
   Symantec_Protection_Engine_Tools_7.9.0.XX_IN.zip\Tools\LiveUpdate_Log_Config\folder into the \etc\symantec directory

2. Edit the following values in the lux.logging.conf file:

   ■ logger.enabled=true
   ■ logger.level=info
   ■ logger.sink=file
   ■ logger.sink.file.filePath= user defined file path

   Note: Ensure that the user defined file path exists.

About Intelligent Update

Symantec provides the latest definition files for download on the Symantec Web site through Intelligent Update packages. Intelligent Update package is updated daily with the most current definition files.

Typically, Intelligent Update packages can be used in isolated networks where latest definitions are not available through LiveUpdate or Rapid Release.

Core 1.5 definition support: From version 7.5.2 onwards, Symantec Protection Engine is integrated with core 1.5 definitions support. You can now update Symantec Protection Engine with the latest Antivirus definitions package.

Based on your operating system on which Symantec Protection Engine is installed, you can download the appropriate core 1.5 Antivirus definitions package for Intelligent Update.

Table 11-4 lists the intelligent update package (core 1.5 definitions) file format for various operating systems.
The name of the Intelligent Update package file for core 1.5 definition support, which changes with each update, uses the following format:

`yyyyymmdd-vvv-core15v5Pbb.exe`

The file name provides the following information:

- `yyyy` year
- `mm` month
- `dd` day
- `vvv` definition version
- `v5` intelligent update version 5 (for Windows files)
- `P` processor (I=Intel, A=Alpha)
- `bb` platform (32=32-bit, 64=64-bit)

For example, `20150503-023-core15v5i64.exe` is the May 03, 2015 build version twenty three, Intel 64-bit update for Windows.

**Note:** Legacy Intelligent Update packages are yet functional.

You can download the appropriate static Intelligent Update package from the following Symantec FTP site:
Based on your operating system on which Symantec Protection Engine is installed, you can download the appropriate Intelligent Update package from the following Symantec FTP site:


Table 11-6 lists the Intelligent Update package file format for different operating systems for full definitions.

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Intelligent Update package file format</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 64-bit</td>
<td>yyyyymmdd-vvv-v5Pbb.exe</td>
<td>20110520-003-v5i64.exe</td>
</tr>
<tr>
<td>Linux 64-bit</td>
<td>yyyyymmdd-vvv-Pbb.sh</td>
<td>20110520-003-i64.sh</td>
</tr>
</tbody>
</table>

Static Intelligent Update package name with the specific file format and link for full definitions is listed in the following table.

Table 11-7 lists the Static Intelligent Update package file format for different operating systems - full definitions.

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Static Intelligent Update package file format</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 64-bit</td>
<td>symcdefsv5i64.exe</td>
</tr>
<tr>
<td>Linux 64-bit</td>
<td>symcdefs-unix64.sh</td>
</tr>
</tbody>
</table>

Note: Static Intelligent Update package download link for full definitions is same as the Static Intelligent Update package core 1.5 definitions support.

Note: Intelligent Update package does not support updating URL definitions updates. You must update URL definitions using LiveUpdate.

See “About LiveUpdate” on page 229.
The name of the Intelligent Update package file, which changes with each update, uses the following format:

```
yyyymmdd-vvv-v5Pbb.exe
```

The file name provides the following information:

- `yyyy`: year
- `mm`: month
- `dd`: day
- `vvv`: definition version
- `v5`: intelligent update version 5 (for Windows files)
- `P`: processor (I=Intel, A=Alpha)
- `bb`: platform (32=32-bit, 64=64-bit)

For example, `20110520-003-v5i64.exe` is the May 20, 2011 build version three, Intel 64-bit update for Windows.

Symantec Protection Engine must be running when you use Intelligent Update package install definitions to ensure that the newer definitions become the active definitions set.

See “Enabling definition updates through Intelligent Update” on page 240.
See “Disabling definition updates through Intelligent Update” on page 242.
See “Updating definitions using Intelligent Update” on page 241.
See “About updating your protection” on page 227.

### Enabling definition updates through Intelligent Update

To update definitions, you must first run a script for your platform to enable Intelligent Update package in Symantec Protection Engine. You need to enable the script only once.
To enable Intelligent Update package for Windows

1. At the command line, change the directory to the Symantec Protection Engine AntiVirus definitions directory.

   The directory is as follows:
   
   C:\Program Files\Symantec\Scan Engine\Definitions\AntiVirus

2. Run the following script to enable Intelligent Update package:
   
   `setup-iu.bat enable`

   The `shadow.iu` file is created in the present working directory. Symantec Protection Engine checks shared definitions once per minute.

   The Intelligent Update package does not work if the `shadow.iu` file is not present in the Symantec Protection Engine AntiVirus definitions directory.

To enable Intelligent Update package for Linux

1. Change directory to the Symantec Protection Engine AntiVirus definitions directory.

   The directory is as follows:
   
   `/opt/SYMCScan/bin/definitions/AntiVirus`

2. Run the following script to enable the Intelligent Update package:
   
   `./setup-iu.sh enable`

   The `shadow.iu` file is created in the present working directory. Symantec Protection Engine checks shared definition once per minute.

   The Intelligent Update package does not work if the `shadow.iu` file is not present in the Symantec Protection Engine AntiVirus definitions directory.

See “Disabling definition updates through Intelligent Update” on page 242.

See “Updating definitions using Intelligent Update” on page 241.

See “About Intelligent Update” on page 237.

Updating definitions using Intelligent Update

To update definitions, you must first run a script for your platform to enable Intelligent Update package in Symantec Protection Engine. You can download the latest virus definitions from the following Symantec FTP site:

To update definitions using Intelligent Update package for Windows

1. Enable the setup-iu.bat script for Intelligent Update package.
2. On your local computer, navigate to the location where Intelligent Update package file is downloaded.
3. Double-click the Intelligent Update package file to update the latest definitions.
   After some processing, Symantec Protection Engine applies the latest definitions. You can verify the virus definition date on the Symantec Protection Engine console home page.

See “About Intelligent Update” on page 237.
See “Enabling definition updates through Intelligent Update” on page 240.
See “Disabling definition updates through Intelligent Update” on page 242.

To update definitions using Intelligent Update package for Linux

1. Enable the setup-iu.sh script for Intelligent Update package.
2. On your local computer, navigate to the location where Intelligent Update package file is downloaded.
3. Execute ./yyyymmdd-vvv-Pbb.sh to extract and apply the AV definitions.
   After some processing, Symantec Protection Engine applies the latest definitions. You can verify the virus definition date on the Symantec Protection Engine console home page.

Disabling definition updates through Intelligent Update

You can use Intelligent Update packages to update definitions in isolated networks.

To disable Intelligent Update package for Windows

1. At the command line, change directory to Symantec Protection Engine AntiVirus definitions directory.
   The directory is as follows:
   C:\Program Files\Symantec\Scan Engine\Definitions\AntiVirus
2. Run the following script to disable the Intelligent Update package:
   setup-iu.bat disable
To disable Intelligent Update package for Linux

1. Change directory to the Symantec Protection Engine AntiVirus definitions directory.

   The directory is as follows:

   /opt/SYMCScan/bin/definitions/AntiVirus

2. Run the following script to disable the Intelligent Update package:

   ./setup-iu.sh disable

See “Enabling definition updates through Intelligent Update” on page 240.

See “Updating definitions using Intelligent Update” on page 241.

See “About Intelligent Update” on page 237.

About Rapid Release

You can configure Symantec Protection Engine to obtain uncertified definition updates with Rapid Release. You can configure Symantec Protection Engine to retrieve Rapid Release definitions every 5 minutes to every 120 minutes.

See “Configuring Rapid Release updates to occur automatically” on page 244.

See “Performing Rapid Release updates on demand” on page 245.

Rapid Release definitions are created when a new threat is discovered. Rapid Release definitions undergo basic quality assurance tests by Symantec Security Response. However, they do not undergo the intense testing that is required for a LiveUpdate release. Symantec updates Rapid Release definitions as needed to respond to high-level outbreaks. Rapid Release definitions might be made available before the LiveUpdate definitions quality assurance process is complete. Rapid Release definitions provide a quick response to new threats and security risks. You can augment Rapid Release definitions later on by more robust detection capabilities in certified definitions.

Warning: Rapid Release definitions do not undergo the same rigorous quality assurance tests as LiveUpdate and Intelligent Update definitions. Symantec encourages users to rely on the full quality-assurance-tested definitions whenever possible. Ensure that you deploy Rapid Release definitions to a test environment before you install them on your network.

If you use a proxy or firewall that blocks FTP communications, the Rapid Release feature does not function. Your environment must allow FTP traffic for the FTP session to succeed.
You can configure Rapid Release to download the definitions from the HTTP server also. See “Configuring Rapid Release to download definitions from HTTP Server” on page 321.

The Rapid Release definitions that are downloaded are automatically selected as the active definitions. However, you can revert to the previous version of the antivirus definition set. The definition set that you choose remains active until the next definition update runs.

See “Rolling back definitions” on page 245.

Rapid Release does not support URL definition updates. You must update URL definitions using LiveUpdate.

See “About LiveUpdate” on page 229.

**Configuring Rapid Release updates to occur automatically**

You can schedule Rapid Release updates to occur automatically at a specified time interval to ensure that Symantec Protection Engine always has the most current definitions. Scheduled Rapid Release updates are disabled by default. To receive automatic Rapid Release updates, you must enable and schedule Rapid Release. When Rapid Release is scheduled, Rapid Release runs at the specified time interval that you select.

See “Configuring Rapid Release updates to occur automatically in the Core server only mode” on page 320.

**Configuring Rapid Release updates to occur automatically**

1. In the console on the primary navigation bar, click **System**.
2. In the sidebar under **Views**, click **Rapid Release Content**.
3. In the content area under **Rapid Release Content**, check **Enable scheduled Rapid Release** to enable automatic downloads of Rapid Release definitions. This option is disabled by default.
4. In the **Rapid Release interval** box, to specify the interval between which you want Symantec Protection Engine to download Rapid Release definitions, do any of the following steps:
   - Type the interval.
   - Click the up arrow or down arrow to select the interval.
You can select any number between 5 minutes and 120 minutes. The default value is 30 minutes.

5 On the toolbar, select one of the following options:

- Save  Saves your changes.
  Use this option to continue making changes in the console until you are ready to apply them.

- Apply  Applies your changes.
  Your changes are not implemented until you apply them.

See “About Rapid Release” on page 243.

Performing Rapid Release updates on demand

You can run Rapid Release on demand to force an immediate update of definitions. If you have scheduled Rapid Release, the next scheduled Rapid Release try occurs at its scheduled time.

To perform Rapid Release updates on demand

1 In the console on the primary navigation bar, click System.
2 In the sidebar under Views, click Rapid Release Content.
3 Under Tasks, click Rapid Release Content.

See “About Rapid Release” on page 243.

Rolling back definitions

Symantec Protection Engine automatically uses the most current set of definitions for scanning. However, if a problem is discovered with the current definitions set, you can revert (rollback) to the previous set of antivirus or URL definitions. You can rollback definitions regardless of the method that is used to obtain the definitions. Symantec Protection Engine supports only one rollback of antivirus and URL definitions sets.

Note: Rollback is not supported for any of the Insight specific content.

Symantec Protection Engine installs with the most current definitions that are available at the time the product is released. After you install the product and activate the licenses, you need to perform a definition update to obtain the most current
definitions. If you discover a problem with the new definitions, you can revert to the definitions that were shipped with the product.

See “About licensing” on page 88.

The LiveUpdate Content page provides information about whether your definition rollback is successful. If the rollback operation fails, it might be because a previous definition set does not exist or because you do not have a valid content license.

To rollback definitions

1. In the console on the primary navigation bar, click System.
2. In the sidebar under Views, click LiveUpdate Content.
3. In the content area under Definition Details, select the definitions set that you want to rollback.
4. In the sidebar under Tasks, click Rollback <definition feature name> Definitions.

See “About definition updates” on page 226.
This chapter includes the following topics:

- About the Core server only mode
- Configuring ICAP options in the Core server only mode
- Configuring Symantec Protection Engine to use the RPC protocol in the Core server only mode
- Adding and removing RPC clients in the Core server only mode
- Configuring the RPC connection options in the Core server only mode
- Notifying a file server when definitions are updated in Core server only mode
- Configuring the antivirus scan policy in the Core server only mode
- Enabling threat detection in the Core server only mode
- Enabling nonviral threat detection in the Core server only mode
- Enabling advanced heuristic scanning in the Core server only mode
- Configuring APK Reputation in the Core server only mode
- Enabling advanced machine learning in the Core server only mode
- Configuring the quarantine server in the Core server only mode
- Configuring file name filtering in the Core server only mode
- Configuring file size filtering in the Core server only mode
- Configuring true type file filtering in the Core server only mode
- Configuring subject line content filtering in the Core server only mode
- Configuring message origin filtering in the Core server only mode
- Configuring Symantec Protection Engine to handle partial container files in the Core server only mode
- Configuring Symantec Protection Engine to handle malformed container files in the Core server only mode
- Configuring Symantec Protection Engine to handle encrypted container files in the Core server only mode
- Customizing notifications in the Core server only mode
- Notifying RPC client users that a threat was found in the Core server only mode
- Enabling Symantec Insight™ in the Core server only mode
- Configuring the Symantec Insight™ aggression level in the Core server only mode
- Excluding files from Insight scanning based on file size in the Core server only mode
- Excluding files from Insight scanning based on SHA256 in the Core server only mode
- Excluding files from Insight scanning based on source IP address in the Core server only mode
- Excluding files from Insight scanning based on source URL in the Core server only mode
- Monitoring scanning requests in the Core server only mode
- Enabling resource consumption logging in the Core server only mode
- Specifying the maximum file or message size to scan in the Core server only mode
- Setting container file limits in the Core server only mode
- Enabling URL filtering in the Core server only mode
- Denying access to URLs in URL categories in the Core server only mode
- Customizing the access denied message in the Core server only mode
- Specifying the log bind address in the Core server only mode
- Specifying the local logging level in the Core server only mode
- Changing the directory where log files are located in the Core server only mode
- Maintaining log files on a shared resource in Windows in the Core server only mode
- Changing the number of log file to be maintained in the Core server only mode
- Enabling statistics reporting in the Core server only mode
- Configuring logging to the Windows Application Event Log in the Core server only mode
- Configuring logging to the Linux Syslog in the Core server only mode
- Activating SMTP alerts in the Core server only mode
- Activating SNMP alerts in the Core server only mode
- Configuring outbreak alerts in the Core server only mode
- Configuring LiveUpdate to occur automatically in the Core server only mode
- Configuring Rapid Release updates to occur automatically in the Core server only mode
- Configuring Rapid Release to download definitions from HTTP Server
- About editing the LiveUpdate XML file

About the Core server only mode

The Symantec Protection Engine user interface requires Java to be installed prior to installing Symantec Protection Engine. From version 7.5.0 onwards, you have the option to install Symantec Protection Engine in the Core server only mode that allows you to administer and configure Symantec Protection Engine using the command-line interface. Since the Core server only mode uses the command-line interface to configure the options, it is independent of Java.

Table 12-1 lists some features that have been adapted to suit the Core server only mode.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration settings</td>
<td>The XMLModifier utility must be used to configure options in Symantec Protection Engine while operating in the Core server only mode.</td>
</tr>
</tbody>
</table>
### Table 12-1

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detailed reporting</td>
<td>Prior to version 7.5.0, reports and logs were generated using the user interface only. Now, you can choose to use the LogConverter utility to generate detailed reports while operating in the Core server only mode. This utility converts the Symantec Protection Engine log files into a readable format. It also converts input log file(s) into text, HTML (-h switch) and CSV (-c switch) formats. The default output format is text.</td>
</tr>
<tr>
<td>Definition updates</td>
<td>In the Core server only mode, you can either update definitions on demand or schedule updates automatically at a specified time interval.</td>
</tr>
</tbody>
</table>

### About XMLModifier tool

The XML files that you can modify are as follows:

- **configuration.xml**
  Contains the protocol settings, resource settings, logging setting, quarantine server setting, and proxy server settings.

- **filtering.xml**
  Contains the settings for URL filtering, container limits and container handling, and file attribute and email attribute handling.

- **liveupdate.xml**
  Contains the LiveUpdate and Rapid Release options.

- **policy.xml**
  Contains an antivirus scan setting, Insight settings, APK reputation settings, and access-denied and notification messages.

Following are the two XML modifier command-line tools for Symantec Protection Engine:

- **XMLModifier.exe**
  A tool used on Windows platforms to modify the XML files.

- **xmlmodifier**
  A tool used on Linux platforms to modify the XML files.

Always run the XMLModifier utility from the installation directory. After you change the settings by using the XMLModifier utility, you must stop and start the Symantec Protection Engine service for the changes to take effect.
XMLModifier options

Use the XML modifier command-line tool of Symantec Protection Engine to modify the XML files.

Note: For boolean values, allowed and recommended values are true or false.

Table 12-2 provides the option commands that you can use with the XML modifier command-line tool of Symantec Protection Engine.

<table>
<thead>
<tr>
<th>Option name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remove</td>
<td>If the XPath specifies an attribute, then that attribute is set to an empty string. If the XPath specifies a group, then the items within that group are removed. If you want to populate a list within the XML document with new items, first remove the whole list. The command is as follows: For Windows: XMLModifier.exe -r &lt;XPath&gt; &lt;XMLfile&gt; For Linux: xmlmodifier -r &lt;XPath&gt; &lt;XMLfile&gt; where &lt;XPath&gt; is the required XPath and &lt;XMLfile&gt; is the XML file name.</td>
</tr>
<tr>
<td>Bulk copy</td>
<td>Use the bulk copy command to insert a list of items that are stored at the XPath. Each item is separated as a new line. The bulk copy command appends the bulk file to the XPath location. Only use this command to insert lists. Each entry must be on a separate line. The command is as follows: For Windows: XMLModifier.exe -b &lt;XPath&gt; bulkfile &lt;XMLfile&gt; For Linux: xmlmodifier -b &lt;XPath&gt; bulkfile &lt;XMLfile&gt; where &lt;XPath&gt; is the required XPath and &lt;XMLfile&gt; is the XML file name.</td>
</tr>
<tr>
<td>Node value</td>
<td>This command sets a node value. The command is as follows: For Windows: XMLModifier.exe -s XPath newvalue &lt;XMLfile&gt; For Linux: xmlmodifier -s &lt;XPath&gt; newvalue &lt;XMLfile&gt; where &lt;XPath&gt; is the required XPath and &lt;XMLfile&gt; is the XML file name. For example, xmlmodifier -s //policies/ThreatPolicies/AntiVirusScanning/@enabled true policy.xml</td>
</tr>
</tbody>
</table>
Encrypt the password (using the AES 256-bit encryption method) and store in specified XPath location

This command encrypts the specified password using the AES 256-bit encryption method and stores it in the specified XPath location. However, only certain parameters support this encryption method in Symantec Protection Engine. Table 12-3 lists the parameters that are encrypted using this method.

The command is as follows:

For Windows: `XMLModifier.exe -k <XPath> <password> <SPE install directory> <XMLfile>

For Linux: `xmlmodifier -k <XPath> <password> <SPE install directory> <XMLfile>

where `<XPath>` is the required XPath, `<password>` is your password, `<SPE install directory>` is the path to the installation directory, and `<XMLfile>` is the XML file name.

Note: Make sure the path to the Symantec Protection Engine installation directory does not end with `/`.

<table>
<thead>
<tr>
<th>Option name</th>
<th>Description</th>
</tr>
</thead>
</table>
| Encrypt the password (using the AES 256-bit encryption method) and store in specified XPath location | This command encrypts the specified password using the AES 256-bit encryption method and stores it in the specified XPath location. However, only certain parameters support this encryption method in Symantec Protection Engine. Table 12-3 lists the parameters that are encrypted using this method. The command is as follows:  

For Windows: `XMLModifier.exe -k <XPath> <password> <SPE install directory> <XMLfile>`  
For Linux: `xmlmodifier -k <XPath> <password> <SPE install directory> <XMLfile>`  

where `<XPath>` is the required XPath, `<password>` is your password, `<SPE install directory>` is the path to the installation directory, and `<XMLfile>` is the XML file name.  

Note: Make sure the path to the Symantec Protection Engine installation directory does not end with `/`. |
| Query | This command returns the value of the node in the XML document with no newline. The command is as follows:  

For Windows: `XMLModifier.exe -q <XPath> <XMLfile>`  
For Linux: `xmlmodifier -q <XPath> <XMLfile>`  

where `<XPath>` is the required XPath and `<XMLfile>` is the XML file name. |
| Query list | This command returns the list of values of the node in the XML document with a newline. The `l` is lowercase, as in list. The command is as follows:  

For Windows: `XMLModifier.exe -l <path> <XMLfile>`  
For Linux: `xmlmodifier -l <path> <XMLfile>`  

where `<XPath>` is the required XPath and `<XMLfile>` is the XML file name. |
Table 12-2  Option commands *(continued)*

<table>
<thead>
<tr>
<th>Option name</th>
<th>Description</th>
</tr>
</thead>
</table>
| Create a new entry in the RPC client list | This command adds a single network attached storage device in the RPC client list. The command is as follows:  
  For Windows: `XMLModifier.exe -c //configuration/ProtocolSettings/RPC/ClientList/items <IP Address of RPC Client / NAS Device> configuration.xml`  
  For Linux: `xmlmodifier -c //configuration/ProtocolSettings/RPC/ClientList/items <IP Address of RPC Client / NAS Device> configuration.xml`  
  **Note:** To list or remove the complete RPC client list, use the `-l` and `-r` option respectively.  
  `XMLModifier.exe -l //configuration/ProtocolSettings/RPC/ClientList/items configuration.xml`  
  `XMLModifier.exe -r //configuration/ProtocolSettings/RPC/ClientList/items configuration.xml` |
| Add local URL categories | This command adds local URL categories. The command is as follows:  
  For Windows: `XMLModifier.exe -a <urlcategory1|urlcategory2|..>`  
  For Linux: `xmlmodifier -a <urlcategory1|urlcategory2|..>`  
  where `<urlcategory>` is the local URL category. |
| Delete local URL categories | This command deletes local URL categories. The command is as follows:  
  For Windows: `XMLModifier.exe -d <urlcategory1|urlcategory2|..>`  
  For Linux: `xmlmodifier -d <urlcategory1|urlcategory2|..>`  
  where `<urlcategory>` is the local URL category. |
| Add URL(s) to local URL category | This command adds URL(s) to local URL category. The command is as follows:  
  For Windows: `XMLModifier.exe -u <urlcategory|url1|url2|..>`  
  For Linux: `xmlmodifier -u <urlcategory|url1|url2|..>`  
  where `<url>` is the url to be added and `<urlcategory>` is the local URL category. |
### Table 12-2  Option commands (continued)

<table>
<thead>
<tr>
<th>Option name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delete URL(s) from local URL category</td>
<td>This command deletes URL(s) from the local URL category. The command is as follows: For Windows: `XMLModifier.exe -v &lt;urlcategory</td>
</tr>
<tr>
<td>Add URL(s) to URL Override List</td>
<td>This command adds URL(s) to URL Override List. The command is as follows: For Windows: `XMLModifier.exe -o &lt;url1</td>
</tr>
<tr>
<td>Delete URL(s) from URL Override List</td>
<td>This command deletes the URL(s) from the URL Override List. The command is as follows: For Windows: `XMLModifier.exe -i &lt;url1</td>
</tr>
</tbody>
</table>

### Table 12-3  Parameters that require password encryption using the AES 256-bit method

<table>
<thead>
<tr>
<th>Parameter name</th>
<th>XPath</th>
<th>Configuration file name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proxy Server Password</td>
<td><code>//configuration/ProxyServerSettings/Password/@value</code></td>
<td><code>configuration.xml</code></td>
</tr>
<tr>
<td>LiveUpdate Server Password</td>
<td><code>//liveupdate/UpdateServer/Password/@value</code></td>
<td><code>liveupdate.xml</code></td>
</tr>
<tr>
<td>Rapid release FTP Password</td>
<td><code>//liveupdate/RapidRelease/FTPSettings/Password/@value</code></td>
<td><code>liveupdate.xml</code></td>
</tr>
</tbody>
</table>
Note: The XMLModifier utility has a dependency on the libxml2 library. If this library is not found, the utility may throw an error. The libxml2 library is already present in the installation directory. However, if the XMLModifier utility is still unable to find the library on UNIX machines, you can add the path, /opt/SYMCScan/bin, to the LD_LIBRARY_PATH environment variable.

---

## Accessing the XML modifier command-line tool

To edit the XML files, use the XML modifier command-line tool. The XML modifier command-line tool is included in the Symantec Protection Engine.zip file. This tool is automatically installed when you install the Symantec Protection Engine.

**To access the XML modifier command-line tool**

- At the command prompt, type the following:

  - For Windows
    ```
    xmlmodifier.exe
    ```
  - For Linux
    ```
    xmlmodifier
    ```

See “About configuration options” on page 366.

## Configuring ICAP options in the Core server only mode

If you select ICAP, you must configure certain options specific to ICAP. You must also configure the ICAP client to work with Symantec Protection Engine. For more information, see the ICAP client documentation.

See Table 12-4 on page 256. describes the configuration options for ICAP.
Table 12-4  Protocol-specific options for ICAP

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bind address</td>
<td>Symantec Protection Engine detects all of the available IP addresses that are installed on the host. By default, Symantec Protection Engine accepts scanning requests on (binds to) all of the scanning IP addresses that it detects. You can configure up to 64 IP addresses as scanning IP addresses. You can specify whether you want Symantec Protection Engine to bind to all of the IP addresses that it detects, or you can restrict access to one or more interfaces. If you do not specify at least one IP address, Symantec Protection Engine binds to all of the scanning IP addresses that it detects. If Symantec Protection Engine fails to bind to any of the selected IP addresses, an event is written to the log as a critical error. Even if Symantec Protection Engine is unable to bind to any IP address, you can access the console. However, scanning functionality is unavailable. See “Logging levels and events” on page 202. <strong>Note:</strong> You can use 127.0.0.1 (the loopback interface) to let only the clients that are running on the same computer connect to Symantec Protection Engine.</td>
</tr>
<tr>
<td>Port number</td>
<td>The port number must be exclusive to Symantec Protection Engine. You must use the same port number for all of the scanning IP addresses that you want to bind to Symantec Protection Engine. The default port number is 1344. If you change the port number, use a number that is equal to or greater than 1024. No other program or service should use this port number.</td>
</tr>
</tbody>
</table>

To configure ICAP protocol

1. Go to the Symantec Protection Engine installation directory.
2. Set the ICAP protocol.

   **Command:**
   
   `xmlmodifier -s //configuration/ProtocolSettings/Protocol/@value ICAP configuration.xml`

   **Allowed values:**
   
   - ICAP
     Enables the ICAP protocol.
   - RPC
Enables the RPC protocol.

**Default value:** ICAP

3 Specify the Bind address.

**Command:**

```
xmlmodifier -s //configuration/ProtocolSettings/ICAP/BindAddress/@value <value>
```

**Allowed values:** Scanning IP addresses that you want to bind to Symantec Protection Engine.

**Default value:** Symantec Protection Engine binds to all interfaces.

4 Specify the port number that the client application uses to pass files to Symantec Protection Engine for scanning.

**Command:**

```
xmlmodifier -s //configuration/ProtocolSettings/ICAP/Port/@value <value>
```

**Allowed values:** Port number that is equal to or greater than 1024. No other program or service should use this port number. You must use the same port number for every scanning IP addresses that you want to bind to Symantec Protection Engine.

**Default value:** 1344

5 Restart the Symantec Protection Engine service.

See “About working with ICAP” on page 97.

See “Verifying, stopping, and restarting the Symantec Protection Engine service on Windows” on page 62.

---

**Configuring Symantec Protection Engine to use the RPC protocol in the Core server only mode**

Before you can configure any of the RPC protocol options, configure Symantec Protection Engine to use the RPC protocol.

To configure Symantec Protection Engine to use the RPC protocol

1 Go to the Symantec Protection Engine installation directory.

2 Set the RPC protocol.

**Command:**
xmlmodifier -s //configuration/ProtocolSettings/Protocol/@value
RPC configuration.xml

**Allowed values:**
- ICAP
  Enables the ICAP protocol
- RPC
  Enables the RPC protocol

**Default value:** ICAP

3 Restart the Symantec Protection Engine service.

See “About working with the RPC protocol” on page 100.

See “About RPC configuration options” on page 101.

---

**Adding and removing RPC clients in the Core server only mode**

You can use a single Symantec Protection Engine to support multiple RPC clients. The supported RPC clients must be located in the same domain as Symantec Protection Engine. You must provide the IP address for each RPC client for which Symantec Protection Engine provides scanning services.

To add an RPC client

1 Go to the Symantec Protection Engine installation directory.

2 Add an RPC client list.

**Command:**

```
xmlder -c
//configuration/ProtocolSettings/RPC/ClientList/items <IP Address of RPC Client / NAS Device> configuration.xml
```

3 Restart the Symantec Protection Engine service.
To remove an RPC client

1. Go to the Symantec Protection Engine installation directory.
2. Remove an RPC client.
   
   **Command:**

   ```
   xmlmodifier -r
   //configuration/ProtocolSettings/RPC/ClientList/items/@value
   configuration.xml
   ```

3. Restart the Symantec Protection Engine service.

See “About working with the RPC protocol” on page 100.
See “About RPC configuration options” on page 101.
See “Configuring Symantec Protection Engine to use the RPC protocol” on page 102.

---

**Configuring the RPC connection options in the Core server only mode**

If your client uses RPC as the communication protocol, you can specify how often you want Symantec Protection Engine to check and retry connections with the RPC client.

**To configure RPC connection options**

1. Go to the Symantec Protection Engine installation directory.
2. Specify the time interval Symantec Protection Engine should check the connection with the RPC client to ensure that the connection is active.

   **Command:**

   ```
   xmlmodifier -s
   //configuration/ProtocolSettings/RPC/RPCConnectionCheckInterval/@value
   <value> configuration.xml
   ```

   **Allowed values:** 0 to 32767

   **Default value:** 20 (seconds)
3 Set the maximum number of times that Symantec Protection Engine should try to re-establish a lost connection with the RPC client.

**Command:**

```
xmlmodifier -s //configuration/ProtocolSettings/RPC/RPCMaxReconnectAttempts/@value <value> configuration.xml
```

**Allowed values:** 0 to 32767

**Default value:** 0

The default setting enables Symantec Protection Engine to try indefinitely to reestablish a connection. Use the default setting if Symantec Protection Engine provides scanning for multiple RPC clients.

4 Restart the Symantec Protection Engine service.

See “About working with the RPC protocol” on page 100.

See “About RPC configuration options” on page 101.

See “Configuring Symantec Protection Engine to use the RPC protocol” on page 102.

---

**Notifying a file server when definitions are updated in Core server only mode**

When the RPC client receives a request for a file from a user, it checks its cache for the file. If the file is not found, the client sends the file to Symantec Protection Engine for scanning. When Symantec Protection Engine returns a clean file to the RPC client, the client stores the file in its cache. The cached file is sent to the user and any subsequent user who requests that file. This process conserves scanning resources.

You can configure Symantec Protection Engine to automatically notify the RPC client that Symantec Protection Engine has new definitions. This notification prompts the RPC client to clear its cache of scanned files, and the process begins again. New requests for files are sent to Symantec Protection Engine for scanning and then cached. Files that are in the cache are sent to the requesting user.

---

**Note:** The process of sending notifications to the file server about definition updates can consume system resources, depending on how often you schedule LiveUpdate. To minimize the impact on performance, you can send the notification on demand, as needed.
You can configure Symantec Protection Engine to automatically notify the network file server of updated definitions after a LiveUpdate occurs. You can also notify the file server on demand, as needed.

To automatically notify a file server when definitions are updated

1. Go to the Symantec Protection Engine installation directory.
2. Configure automatic antivirus update notifications.

   **Command:**
   ```bash
   xmlmodifier -s
   //configuration/ProtocolSettings/RPC/AutomaticSendVirusUpdatesEnabled/@value
   <value> configuration.xml
   
   Allowed values:
   - true
     Automatically sends antivirus update notifications to the file server.
   - false
     Disables the automatically send antivirus update notifications to the file server.
   
   Default value: false
   
   3. Restart the Symantec Protection Engine service.

See “About working with the RPC protocol” on page 100.

**Configuring the antivirus scan policy in the Core server only mode**

You can configure Symantec Protection Engine to do one of the following when an infected file is found:

To configure the antivirus scan policy

1. Go to the Symantec Protection Engine installation directory.
2. Enable the antivirus scanning.

   **Command:**
   ```bash
   xmlmodifier -s
   //policies/ThreatPolicies/AntiVirusScanning/@enabled <value>
   policy.xml
   
   Allowed values:
   - true
Enables antivirus scanning.

- false
  Enables antivirus scanning.

**Default value:** true

3 Configure Symantec Protection Engine to do one of the following when an infected file is found.

**Command:**

```
xmlmodifier -s
//policies/ThreatPolicies/Actions/AVActionPolicy/@value <value> policy.xml
```

**Allowed values:**

- 0 - Scan only
- 1 - Scan and repair
- 2 - Scan and repair or delete
- 3 - Scan and delete

**Default value:** 2 - Scan and repair or delete

---

**Note:** You must select Scan and repair or delete if you plan to quarantine the infected files that cannot be repaired. See “About quarantining files in Symantec Protection Engine” on page 119.

4 Restart the Symantec Protection Engine service.

---

**Enabling threat detection in the Core server only mode**

Symantec Protection Engine can detect viral and nonviral threats, such as viruses, Trojan horses, worms, and security risks in all major file types. For example, Windows, DOS, Microsoft Word, and Microsoft Excel files. To detect threats, you must enable the threat detection capability in the Symantec Protection Engine.

Symantec Protection Engine uses Bloodhound heuristic technology to detect new and unknown threats. You can customize Bloodhound Detection from zero protection to a high level of protection. However, a high level of protection increases protection of your network but it decreases the server performance. At low levels of protection, server performance is unaffected but an unknown threat might escape detection.
In most cases, the default setting (medium) is appropriate. Symantec Protection Engine also gives you an option to quarantine threats. You can quarantine threats if you have configured quarantine server in Symantec Protection Engine.

See "How Symantec Protection Engine detects risks" on page 112.

See "Ways to test threat detection capabilities" on page 116.

You must have a valid antivirus scanning license to scan for threats and a valid content license to update virus definitions. If you upgrade from a previous version and your licenses are current, Symantec Protection Engine automatically recognizes these licenses.

To enable threat detection in Symantec Protection Engine

1. Go to the Symantec Protection Engine installation directory.
2. Enable virus scanning.
   
   **Command:**
   ```
   xmlmodifier -s //policies/ThreatPolicies/AntiVirusScanning/@enabled true policy.xml
   ```

   **Allowed values:**
   - true
     Enables antivirus scanning.
   - false
     Disables antivirus scanning.

   **Default value:** true

3. Select the appropriate Bloodhound Detection level.
   
   **Command:**
   ```
   xmlmodifier -s //policies/ThreatPolicies/AntiVirusScanning/BloodhoundLevel/@value <value> policy.xml
   ```

   **Allowed values:**
   - 0
     Off: Disables the heuristic based file scanning.
   - 1
     Low: Optimizes the server performance, but might not detect potential threats.
   - 2
Medium: Provides a balance between threat detection and server performance.

- 3
  High: Increases the detection of threats, but might affect the server performance.

**Default value:** 2

4 Select the scan policy to handle infected files.

**Command:**

```
xmlmodifier -s //policies/ThreatPolicies/Actions/AVActionPolicy/@value <value> policy.xml
```

**Allowed values:**

- 0
  Scan only: Denies the access to the infected file but does nothing to the infected file.

- 1
  Scan and repair files: Tries to repair infected files but does nothing to the files that cannot be repaired. Security risks cannot be repaired.

- 2
  Scan and repair or delete: Tries to repair infected files and deletes any unrepairable files from archive files. Security risks cannot be repaired.

- 3
  Scan and delete: Deletes all infected files without trying to repair them, including the files that are embedded in archive files.

**Default value:** 2

5 Enable quarantine to quarantine the threats.

```
xmlmodifier -s //policies/ThreatPolicies/Actions/Quarantine/@value true policy.xml
```

**Allowed values:**

- true:
  Enables the quarantine.

- false:
  Disables the quarantine.

**Default value:** false

6 Restart the Symantec Protection Engine service.
Enabling nonviral threat detection in the Core server only mode

If your client uses the ICAP protocol or the RPC protocol, you can enable the detection of one or more types of nonviral threats.

Nonviral threats are the programs that do any of the following actions:

■ Provide unauthorized access to computer systems
■ Compromise data integrity, privacy, confidentiality, or security
■ Present some type of disruption or nuisance

These programs can put your employees and your organization at risk for identity theft or fraud if they can do any of the following actions:

■ Log keystrokes
■ Capture email and instant messaging traffic
■ Harvest personal information, such as passwords and logon identifications

Nonviral threats can be introduced into your system unknowingly when users do any of the following tasks:

■ Visit a Web site
■ Download shareware or freeware software programs
■ Click links or attachments in email messages
■ Use instant messaging clients
■ Agree to an end user license agreement from another software program

Symantec Protection Engine scans for nonviral threats in all types of content, such as email messages and Web content. Symantec Protection Engine can also scan POST transactions for nonviral threats. Symantec Protection Engine can only perform nonviral threat scanning when you enable virus scanning.

See “Enabling threat detection in Symantec Protection Engine” on page 114.

If a nonviral threat is detected, Symantec Protection Engine applies the scan policy that you configured. Symantec Protection Engine also gives you an option to quarantine nonviral threats also. You can quarantine threats if you have configured quarantine server in Symantec Protection Engine.
To enable nonviral threat detection

1. Go to the Symantec Protection Engine installation directory.
2. Enable nonviral threat detection.

   **Command:**

   ```
   xmlmodifier -s //policies/ThreatPolicies/AntiVirusScanning/SecurityRiskScanning/@enabled true policy.xml
   ```

   **Allowed values:**
   - true
     Enables security risk detection.
   - false
     Disables security risk detection.

   **Default value:** true

3. Restart the Symantec Protection Engine service.

---

**Note:** Nonviral threat detection is available only when virus scanning is enabled.

You must restart the Symantec Protection Engine service after the changes.

See “Configuring ICAP options” on page 98.

See “About licensing” on page 88.

---

## Enabling advanced heuristic scanning in the Core server only mode

Advanced Heuristics applies a detection method that is more aggressive than the standard detection and hence leads to better protection. On enabling this feature, there may be a slight decrease in performance and a slight increase in false positives. It is recommended to enable this feature when there is a suspected infection outbreak in the network. You can disable this feature after the outbreak has been resolved and is under control.

**To enable advanced heuristic scanning in Symantec Protection Engine**

1. Go to the Symantec Protection Engine installation directory.
2. Enable advanced heuristic scanning.

   **Command:**

   ```
   ```
xmlmodifier -s //policies/ThreatPolicies/
AntiVirusScanning/AdvancedHeuristicsScanning/@enabled true
policy.xml

**Allowed values:**

- **true**
  - Enables advanced heuristics scanning.
- **false**
  - Disables advanced heuristics scanning.

**Default value:** false

3 Restart the Symantec Protection Engine service.

See “Enabling nonviral threat detection in Symantec Protection Engine” on page 117.

## Configuring APK Reputation in the Core server only mode

APK Reputation feature is enabled by default. You can configure the APK Reputation settings in the Core server only mode.

### To configure APK Reputation

1 Go to the Symantec Protection Engine installation directory.

2 Enable APK Reputation.

   **Command:**
   
   xmlmodifier -s //policies/ThreatPolicies/APKReputation/@enabled true policy.xml

**Allowed values:**

- **true**
  - APK Reputation feature is enabled
- **false**
  - APK Reputation feature is disabled

**Default value:** true

3 Configure threshold security rating value.

   This parameter sets the threshold security rating. APK files having security rating above or equal to the configured threshold security rating value will be blocked or deleted.

   **Command:**
xmlmodifier -s
//policies/ThreatPolicies/APKReputation/ThresholdSecurityRating/@value <value> policy.xml

**Allowed values:** 0 to 6
- 0 - High Good
- 1 - Medium Good
- 2 - Low Good
- 3 - Neutral
- 4 - Low Bad
- 5 - Medium Bad
- 6 - High Bad

**Default value:** 4

Specify how Symantec Protection Engine should handle the APK files that have the security rating above or equal to the configured threshold value.

**Command:**
xmlmodifier -s
//policies/ThreatPolicies/Actions/APKReputationActionPolicy/@value <value> policy.xml

**Allowed values:**
- 1
  - Blocks the file.
- 2
  - Deletes the file.

**Default value:** 1 - Blocks the file

5 Restart the Symantec Protection Engine service.

See “About Android Application (APK) Reputation” on page 193.

---

**Enabling advanced machine learning in the Core server only mode**

You must use XMLModier tool to enable or disable advanced machine learning feature as it is not available on Symantec Protection Engine console.
To enable advanced machine learning in the Core server only mode

1. Go to the Symantec Protection Engine installation directory.
2. Enable advanced machine learning.
   
   **Command:**
   
   ```
   xmlmodifier -s //policies/ThreatPolicies/AntiVirusScanning/AdvancedMachineLearning/@enabled true policy.xml
   ```
   
   **Allowed values:**
   
   - **true**
     Enables the advanced machine learning
   - **false**
     Disables the advanced machine learning
3. Start the Symantec Protection Engine service.

See “About advanced machine learning” on page 144.

Configuring the quarantine server in the Core server only mode

If you plan to quarantine the files that might contain threats or malicious code, configure Symantec Protection Engine to quarantine files. Also provide the host name or IP address for the computer on which Symantec Central Quarantine Server is installed.

To configure quarantine server in Symantec Protection Engine

1. Go to the Symantec Protection Engine installation directory.
2. Enable the quarantine settings.

   **Command:**
   
   ```
   xmlmodifier -s //configuration/QuarantineServerSettings/@enabled true configuration.xml
   ```
   
   **Allowed values:**
   
   - **false**
     Disables quarantine.
   - **true**
     Enables quarantine.

   **Default value: false**
3 Specify the quarantine server name.

Command:

```
xm1modifier -s //configuration/QuarantineServer
Settings/ServerName/@value <server name> configuration.xml
```

Allowed values:

- Hostname or IP address for the computer on which Symantec Central Quarantine Server is installed.

4 Specify the quarantine server port.

```
xm1modifier -s //configuration/QuarantineServer
Settings/ServerPort/@value <value> configuration.xml
```

For example,

```
xm1modifier -s //configuration/QuarantineServer
Settings/ServerPort/@value 4200 configuration.xml
```

Allowed values:

- TCP/IP port number that Symantec Protection Engine uses to pass files to Symantec Central Quarantine.

5 Restart the Symantec Protection Engine service.

See “About quarantining files in Symantec Protection Engine” on page 119.
See “Enabling threat detection in Symantec Protection Engine” on page 114.
See “Configuring Symantec Protection Engine to handle malformed container files” on page 132.
See “Configuring Symantec Protection Engine to handle encrypted container files” on page 134.

### Configuring file name filtering in the Core server only mode

If your client uses the ICAP protocol, you can filter files by file name to protect your network during an outbreak. For example, if you know the file name of a new email borne threat, you can use this information to block infected email messages.

You can configure Symantec Protection Engine to handle the file in one of the following ways:
Block access to the file or the message
Blocks access to any top level file that matches the file name. If a container file or email message contains a file or attachment that matches the file name, access to the entire container or message is blocked.

Delete the file or the attachment
Deletes any file that matches the file name and logs the violation. Symantec Protection Engine deletes any attachments within an email message that match the file name. Attachments that do not match the file name are not deleted and are delivered with the message. If you activate the mail message update feature, the message indicates that an attachment has been deleted due to a policy violation.

Symantec Protection Engine deletes any embedded files that match the specified file name within a container file that contains multiple files. The embedded files that do not match the specified file name are not deleted. Deleted files are replaced with a replacement file, DELETED.TXT, which indicates the reason that the file was deleted.

See “Customizing notifications in Symantec Protection Engine” on page 135.

Use wildcard characters if you are unsure of an exact file name or to block all file attachments with a specific extension. For example, you can use the wildcard *virus* to block all attachments with the word virus in the file name.

**Note:** If your client uses the antivirus-only application programming interface (API), file name violations are reported to the client in the server's response as email policy violations. If you use the extended API or have a standard ICAP implementation, this type of violation is reported as a file violation.

To configure file name filtering in Symantec Protection Engine
1. Go to the Symantec Protection Engine installation directory.
2. Enable filtering by file name.
   **Command:**
   ```bash
   xmlmodifier -s //filtering/FileAttribute/FileNamesEnabled/@value true filtering.xml
   ```
   **Allowed values:**
   - true
     Enable file name filtering.
   - false
     Disable file name filtering.
Default value: true

3 Create a text file and type the file names that you want to filter. Type one entry per line. Search strings are not case-sensitive.

Command:

xmlmodifier -b //filtering/FileAttribute/DenyFileNames/items<filename> filtering.xml

For example, xmlmodifier -b
//filtering/FileAttribute/DenyFileNames/items sample.txt
filtering.xml

Allowed values:
A text file with the list of the file names that you want to filter.

4 Specify an action to block or delete the file.

Select one of the options to specify how you want Symantec Protection Engine to handle the messages that contain an attachment with that file name:

Command:

xmlmodifier -s //filtering/FileAttribute/DeleteFileNames/@value <value> filtering.xml

Allowed values:

- true
  Delete the file or attachment.

- false
  Block access to the file or the message.

Default value: false

5 Restart the Symantec Protection Engine service.

See “About preventing potential threats in Symantec Protection Engine” on page 121.
See “Configuring file size filtering in Symantec Protection Engine” on page 124.
See “Configuring subject line content filtering in Symantec Protection Engine” on page 126.
See “Configuring message origin filtering in Symantec Protection Engine” on page 128.
Configuring file size filtering in the Core server only mode

If your client uses the ICAP protocol, you can filter files based on their sizes. For example, suppose you know the exact size of new email borne threat. You can use this information to block any email messages that match this size.

You can configure Symantec Protection Engine to handle the file in one of the following ways:

- **Block access to the file or the message**
  - Blocks access to any top level file that matches the file size.
  - If a container file or email message contains a file or attachment that matches the specified file size, Symantec Protection Engine blocks the entire container or message.

- **Delete the file or attachment**
  - Deletes any files that match the specified file size and logs the violation.
  - Symantec Protection Engine deletes any attachments within an email message that match a specified file size. Attachments that do not match the specified file size are delivered with the message. If you activate the mail message update feature, the mail message indicates that an attachment has been deleted due to a file policy violation.
  - Symantec Protection Engine deletes any embedded files within a container file that contains multiple files that match the specified file size. The embedded files that do not match the specified file size are not deleted. Deleted files are replaced with a replacement file, DELETED<N>.TXT (where N denotes the sequence number), which indicates the reason that the file was deleted.
  - See "Customizing notifications in Symantec Protection Engine" on page 135.

To configure file size filtering in Symantec Protection Engine

1. Go to the Symantec Protection Engine installation directory.
2. Enable filtering by file size.

   **Command:**
   ```bash
   xmlmodifier -s //filtering/FileAttribute/FileSizesEnabled/@value true filtering.xml
   ```

   **Allowed values:**
   - `true`
     - Enable file size filtering.
   - `false`
Disable file size filtering.

**Default value:** true

3 Create a text file and type the file sizes that you want to filter. Type one entry per line.

**Command:**

```bash
xmlmodifier -b //filtering/FileAttribute/DenyFileSizes/items <filename> filtering.xml
```

For example, `xmlmodifier -b //filtering/FileAttribute/DenyFileSizes/items sample.txt filtering.xml`

**Allowed values:**
A text file with the list of the file sizes that you want to filter.

4 Specify an action to block or delete the file.

Specify how you want Symantec Protection Engine to handle the messages that contain an attachment with that file size:

**Command:**

```bash
xmlmodifier -s //filtering/FileAttribute/DeleteFileSizes/@value true filtering.xml
```

**Allowed values:**

- true
  - Delete the file or attachment.

- false
  - Block access to the file or the message

**Default value:** false

5 Restart the Symantec Protection Engine service.

See “About preventing potential threats in Symantec Protection Engine” on page 121.

See “Configuring file name filtering in Symantec Protection Engine” on page 122.

See “Configuring subject line content filtering in Symantec Protection Engine” on page 126.

See “Configuring message origin filtering in Symantec Protection Engine” on page 128.
Configuring true type file filtering in the Core server only mode

You can configure Symantec Protection Engine to handle the file based on its type. It blocks access to any top level file that matches the file type. If a container file or email message contains a file or attachment that matches the file type, access to the entire container or message is blocked.

You can use wildcard characters for the files based on their categories to block the files. For example, you can use the wildcard image/* to block all files that fall under the image category.

**Note:** Configuration of the file true type filtering is supported only on ICAP protocol.

To configure file type filtering in Symantec Protection Engine

1. Go to the Symantec Protection Engine installation directory.
2. Enable filtering by file type.

   **Command:**
   ```bash
   xmlmodifier -s //filtering/FileAttribute/FileTypeFilteringEnabled/@value true filtering.xml
   ```

   **Allowed values:**
   - **true**
     Enables true type file filtering in Symantec Protection Engine.
   - **false**
     Disables true type file filtering in Symantec Protection Engine.

   **Default value:** false
3 Create a text file and type the file types that you want to filter. Type one entry per line.

Command:

xmlmodifier -b //filtering/FileAttribute/DenyFileTypes/items <filename> filtering.xml

For example, xmlmodifier -b //filtering/FileAttribute/DenyFileTypes/items @value "audio/mp3" filtering.xml

Allowed values:
A text file with the list of the file types that you want to filter.

4 Restart the Symantec Protection Engine service.

Configuring subject line content filtering in the Core server only mode

If your client uses the ICAP protocol, you can configure Symantec Protection Engine to block messages by the subject line. You can use this feature to handle new threats for which a threat definition has not been created. You can also use this feature to filter mail messages for inappropriate or confidential information or potential spam.

Symantec Protection Engine scans the subject lines of incoming mail messages for the text string that you specify. You can use wildcard characters when you are not sure of the exact subject line. Symantec Protection Engine ignores any white space (tabs or spaces) at the beginning of the subject line. It also ignores any white space that you enter at the beginning of your text string.

To configure subject line content filtering in Symantec Protection Engine

1 Go to the Symantec Protection Engine installation directory.

2 Enable filtering by subject line.

Command:

xmlmodifier -s //filtering/EmailAttribute/DenySubjects/@value true filtering.xml

Allowed values:

- true
  - Enable filtering by subject line.
- false
Disable filtering by subject line.

**Default value:** false

3. Create a text file and type the subject line or text string in the subject line that you want to block.

Type as many subject lines to block as needed. Type one entry per line. Search strings are not case-sensitive.

**Command:**

```
xmldiff -b //filtering/EmailAttribute/DenySubjectsList/items <file name> filtering.xml
```

**For example,** `xmldiff -b //filtering/EmailAttribute/DenySubjectsList/items sample.txt filtering.xml`

**Allowed values:**
- A text file with the list of the subject lines.

4. Block the messages with empty subject lines.

**Command:**

```
xmldiff -s //filtering/EmailAttribute/DenyEmptySubjects/@value true filtering.xml
```

**Allowed values:**
- true
  - Block messages with empty subject lines.
- false
  - Allow messages with empty subject lines.

**Default value:** false

5. Restart the Symantec Protection Engine service.

See “About preventing potential threats in Symantec Protection Engine” on page 121.

See “Configuring file name filtering in Symantec Protection Engine” on page 122.

See “Configuring file size filtering in Symantec Protection Engine” on page 124.

See “Configuring message origin filtering in Symantec Protection Engine” on page 128.
Configuring message origin filtering in the Core server only mode

If your client uses the ICAP protocol, you can configure Symantec Protection Engine to block mail messages from a specific domain or email address. The domain name search string that you enter is matched against the addresses in the From header of the email message. If the search string matches an address, the message is rejected.

The following table contains examples of the ways that you can define the email addresses and domains that you want to block:

| **name@example.symantecdomain.com** | Blocks mail from a single email address. You can use the wildcard characters $ and * in the user portion of the name. The $ wildcard character matches a single character. The * wildcard character matches zero or more characters. You cannot use both wildcard characters in the same entry. For example, *example$s@internet.domain is not supported. You cannot use wildcard characters in subdomain or domain addresses. The subdomain and domain must match exactly. |
| **@example.symantecdomain.com** | Blocks all mail from a specific domain and subdomain address. For example, mail from name@example.symantecdomain.com is allowed. You must precede the address with an @ symbol to ensure that only mail from that specific address is blocked. The use of wildcard characters in subdomain or domain addresses is not supported. |
| **.symantecdomain.com** | Blocks all mail from an entire domain, including any subdomains. For example, mail from example.symantecdomain.com or internet.symantecdomain.com would be blocked. You must precede the domain address with a period to ensure that any subdomains are blocked. You cannot use wildcard characters in subdomain or domain addresses. |

To configure message origin filtering in Symantec Protection Engine

1. Go to the Symantec Protection Engine installation directory.
2. Enable message origin filtering.
Command:
xmlmodifier -s //filtering/EmailAttribute/DenyBlackLists/@value true filtering.xml

Allowed values:
- true
  Enables message origin filtering in Symantec Protection Engine.
- false
  Disables message origin filtering in Symantec Protection Engine.

Default value: false

Create a text file and type a domain address or email address. Type one per line. You can enter up to 5000 addresses. Search strings are not case-sensitive.

Command:
xmlmodifier -b //filtering/EmailAttribute/BlackListAddresses/items <file name> filtering.xml

For example, xmlmodifier -b //filtering/EmailAttribute/BlackListAddresses/items sample.txt filtering.xml

Allowed values:
A text file with the list of blacklisted email or domain addresses that you want to filter.

Restart the Symantec Protection Engine service.

See “About preventing potential threats in Symantec Protection Engine” on page 121.
See “Configuring file name filtering in Symantec Protection Engine” on page 122.
See “Configuring file size filtering in Symantec Protection Engine” on page 124.
See “Configuring subject line content filtering in Symantec Protection Engine” on page 126.

Configuring Symantec Protection Engine to handle partial container files in the Core server only mode

Some email software applications break down large messages into a number of smaller, more manageable messages for transmission. These messages are typically transmitted separately and reassembled before delivery to the recipient. Symantec Protection Engine is unable to scan partial messages. You can configure Symantec Protection Engine to handle partial container files.
To configure Symantec Protection Engine to handle partial container files

1. Go to the Symantec Protection Engine installation directory.

2. Deny partial MIME container files.

   **Command**
   
   `xmlmodifier -s //filtering/Container/DenyPartialMIME/@actionpolicy 1 filtering.xml`

   **Allowed values**

   - 0
     
     Allows access to the partial MIME container files.

   - 1
     
     Denies access to the partial MIME container files.

   **Default value**

   1

Symantec Protection Engine must receive a MIME-encoded message in its entirety to scan it for threats. Some email software applications break down large messages into a number of smaller, more manageable messages for transmission. These messages are typically transmitted separately and reassembled before delivery to the recipient. Because the message is broken down into several partial messages, the entire message (including all attachments) is not available to Symantec Protection Engine for scanning. Symantec Protection Engine is configured by default to reject partial messages because they cannot be effectively scanned for threats.

See “About container files in Symantec Protection Engine” on page 130.

See “Configuring Symantec Protection Engine to handle malformed container files” on page 132.

See “Configuring Symantec Protection Engine to handle encrypted container files” on page 134.

**Configuring Symantec Protection Engine to handle malformed container files in the Core server only mode**

Malformed container files are unscannable in Symantec Protection Engine. If you want to protect your network from threats of malformed container files, configure Symantec Protection Engine to handle unscannable malformed container files.
To configure Symantec Protection Engine to handle malformed container files

1. Go to the Symantec Protection Engine installation directory.

2. Enable malformed container file handling.

   Command:
   ```
   xmlmodifier -s
   //filtering/Container/MalformedContainersHandling/@enabled true
   filtering.xml
   ```

   **Allowed values:**
   - true
     Enables options to handle malformed container files.
   - false
     Disables options to handle malformed container files.

   **Default value:** true

3. Specify how Symantec Protection Engine should handle malformed container files.

   Command:
   ```
   xmlmodifier -s
   //filtering/Container/MalformedContainersHandling/Actions/
   MalformedContainersActionPolicy/@value <value> filtering.xml
   ```

   **Allowed values:**
   - 0
     Generates a log entry. Symantec Protection Engine only logs instances of malformed container files.
   - 1
     Blocks the malformed container files and generates a log entry.
   - 2
     Deletes the malformed container files and generates a log entry.

   **Default value:** 1


   Command:
   ```
   xmlmodifier -s
   //filtering/Container/MalformedContainersHandling/Actions/
   ContinueProcessingInMalformedBlockPolicy/@value true
   filtering.xml
   ```

   **Allowed values:**
true
Continues the scanning of the container file that is blocked.

false
Stops the scanning of the container file that is blocked.

**Default value:** false

5 Quarantine the malformed files.

**Command:**
```
xmlmodifier -s //filtering/Container/MalformedContainersHandling/Actions/Quarantine/@value
true filtering.xml
```

**Allowed values:**

- **true**
  Quarantines the malformed files.

- **false**
  Does not quarantine the malformed files.

**Default value:** false

6 Restart the Symantec Protection Engine service.

See “About container files in Symantec Protection Engine” on page 130.

See “Configuring Symantec Protection Engine to handle partial container files” on page 131.

See “Configuring Symantec Protection Engine to handle encrypted container files” on page 134.

See “Configuring the quarantine in Symantec Protection Engine” on page 120.

---

### Configuring Symantec Protection Engine to handle encrypted container files in the Core server only mode

Encrypted files are unscannable in Symantec Protection Engine. If you want to protect your network from threats of encrypted container files, configure Symantec Protection Engine to handle unscannable encrypted container files.

**To configure file type filtering in Symantec Protection Engine**

1. Go to the Symantec Protection Engine installation directory.

2. Enable encrypted container file handling.

**Command:**
xmlmodifier -s
//filtering/Container/EncryptedContainersHandling/@enabled true filtering.xml

Allowed values:

- true
  Enables options to handle encrypted container files.

- false
  Disables options to handle encrypted container files.

Default value: true

Specify how you want Symantec Protection Engine to handle encrypted container files.

Command:
xmlmodifier -s
//filtering/Container/EncryptedContainersHandling/Actions/EncryptedContainersActionPolicy/@value <value> filtering.xml

Allowed values:

- 0
  Generates a log entry. Symantec Protection Engine only logs instances of encrypted container files.

- 1
  Blocks the encrypted container files and generates a log entry.

- 2
  Deletes the encrypted container files and generates a log entry.

Default value: 0

Continue scanning of the blocked encrypted container file.

Command:
xmlmodifier -s
//filtering/Container/EncryptedContainersHandling/Actions/ContinueProcessingInEncryptedBlockPolicy/@value true filtering.xml

Allowed values:

- true
  Continues the scanning of the encrypted file that is blocked.

- false
  Stops the scanning of the encrypted file that is blocked.
**Default value**: false

5. Quarantine the encrypted files.

Command:

```
xmlmodifier -s //filtering/Container/EncryptedContainersHandling/Actions/Quarantine/@value true filtering.xml
```

**Allowed values**:

- **true**
  - Quarantines the encrypted files.
- **false**
  - Does not quarantine the encrypted files.

**Default value**: false

6. Restart the Symantec Protection Engine service.

See “About container files in Symantec Protection Engine” on page 130.

See “Configuring Symantec Protection Engine to handle partial container files” on page 131.

See “Configuring Symantec Protection Engine to handle malformed container files” on page 132.

See “Configuring the quarantine in Symantec Protection Engine” on page 120.

---

**Customizing notifications in the Core server only mode**

You can configure Symantec Protection Engine to customize messages to users to notify them when a file is infected, repaired, denied access to, malformed, encrypted, or deleted. You can add the text to the body of an infected MIME-encoded message or to the body of a replacement file for a deleted attachment.

Symantec Protection Engine attaches a text file to the email message in the place of each attachment that is deleted because it cannot be repaired. The text file that is inserted is called `DELETED<N>.TXT`, where N is a sequence number. For example, if two attachments are deleted, the replacement files are called `DELETED0.TXT` and `DELETED1.TXT`.

When you use ICAP, Symantec Protection Engine displays an HTML text message to the user when a requested file is blocked. Access to a file is blocked when the file contains a threat and cannot be repaired.

*Table 12-5* describes the types of notification messages that you can customize.
Table 12-5  User notification messages

<table>
<thead>
<tr>
<th>Type of notification</th>
<th>Default text</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deleted file</td>
<td>File: ${FILE_NAME} was infected with ${THREAT_NAME} (${THREAT_ID}). File ${QUARANTINED}. File was deleted.</td>
</tr>
<tr>
<td>Repaired file</td>
<td>File: ${FILE_NAME} was infected with ${THREAT_NAME} (${THREAT_ID}). File ${QUARANTINED}. File was repaired.</td>
</tr>
<tr>
<td>Infected file</td>
<td>File: ${FILE_NAME} was infected with ${THREAT_NAME} (${THREAT_ID}). File ${QUARANTINED}. File is still infected</td>
</tr>
<tr>
<td>Total threat found</td>
<td>This email message was infected. ${TOTAL_THREATS} number of threats were found.</td>
</tr>
<tr>
<td>Denied file size</td>
<td>The file attached to this email was removed because the file size is not allowed. File attachment: ${FILE_NAME}. Matched file size: ${FILE_SIZE}.</td>
</tr>
<tr>
<td>Denied file names</td>
<td>The file attached to this email was removed because the file name is not allowed. File attachment: ${FILE_NAME}. Matched pattern: ${MATCHING_FILENAME_ENTRY}.</td>
</tr>
<tr>
<td>Encrypted file</td>
<td>The encrypted container attached to this email was removed. File attachment: ${FILE_NAME}. File ${QUARANTINED}.</td>
</tr>
<tr>
<td>Malformed file</td>
<td>The malformed container attached to this email was removed. File attachment: ${FILE_NAME}. File ${QUARANTINED}.</td>
</tr>
<tr>
<td>Web browser</td>
<td>The content you just requested contains ${THREAT_NAME} and was blocked by the Symantec Protection Engine based on local administrator settings. Contact your local administrator for further information.</td>
</tr>
<tr>
<td>APK violation</td>
<td>File: ${FILE_NAME} violates APK reputation policy. File ${QUARANTINED}. File was deleted.</td>
</tr>
</tbody>
</table>

You can configure Symantec Protection Engine to customize Insight messages to notify users when a file is infected, replaced, or deleted. You can add the text to the body of an infected MIME-encoded message or to the body of a replacement file for a deleted attachment.

Table 12-6 describes the types of Insight notification messages that you can customize.
Table 12-6 Insight notification messages

<table>
<thead>
<tr>
<th>Type of notification</th>
<th>Default text</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deleted file</td>
<td>File: ${FILE_NAME} was infected with ${THREAT_NAME} (${THREAT_ID}). File ${QUARANTINED}. File was deleted.</td>
</tr>
<tr>
<td>Infected file</td>
<td>File: ${FILE_NAME} was infected with ${THREAT_NAME} (${THREAT_ID}). File ${QUARANTINED}. File is still infected.</td>
</tr>
</tbody>
</table>

Table 12-7 lists the variables that you can use to customize your notifications.

Table 12-7 Notification variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>${FILE_NAME}</td>
<td>The name of the infected file.</td>
</tr>
<tr>
<td>${FILE_SIZE}</td>
<td>The size of the file that violates the maximum file size threshold.</td>
</tr>
<tr>
<td></td>
<td>See “Configuring file size filtering in Symantec Protection Engine” on page 124.</td>
</tr>
<tr>
<td>${THREAT_NAME}</td>
<td>The name of the threat.</td>
</tr>
<tr>
<td>${THREAT_ID}</td>
<td>The threat identification number.</td>
</tr>
<tr>
<td>${QUARANTINED}</td>
<td>Indicates whether a file was quarantined.</td>
</tr>
<tr>
<td></td>
<td>See “About quarantining files in Symantec Protection Engine” on page 119.</td>
</tr>
<tr>
<td>${TOTAL_THREATS}</td>
<td>The total number of risks that are detected in the MIME message.</td>
</tr>
<tr>
<td>${MATCHING_FILENAME_ENTRY}</td>
<td>The file name pattern that triggered the violation.</td>
</tr>
<tr>
<td></td>
<td>See “Configuring file name filtering in Symantec Protection Engine” on page 122.</td>
</tr>
</tbody>
</table>

To customize user notifications in Symantec Protection Engine

1. Go to the Symantec Protection Engine installation directory.
2. Enable the user notifications.
   
   **Command:**
   
   ```
   xmlmodifer -s
   //policies/ThreatPolicies/Notifications/NotificationTextAtTop/@value
   true policy.xml
   ```
Allowed values:

- **true**
  Adds notifications at the top of the message.

- **false**
  Does not add notifications at the top of the message.

**Default value:** false

3 Customize the notification for access denied message.

**Command:**
```
xmlmodifier -s //policies/ThreatPolicies/Notifications/AccessDeniedMessage/@value <text> policy.xml
```

**Default value:** The content you just requested contains ${THREAT_NAME} and was blocked by the Symantec Protection Engine based on local administrator settings. Contact your local administrator for further information.

4 Customize the notification for file deleted notification.

**Command:**
```
xmlmodifier -s //policies/ThreatPolicies/Notifications/FileDeletedNotificationText/@value <text> policy.xml
```

**Default value:** File: ${FILE_NAME} was infected with ${THREAT_NAME} (${THREAT_ID}). File ${QUARANTINED}. File was deleted.

5 Customize the notification for file repaired message.

**Command:**
```
xmlmodifier -s //policies/ThreatPolicies/Notifications/FileRepairedNotificationText/@value <text> policy.xml
```

**Default value:** File: ${FILE_NAME} was infected with ${THREAT_NAME} (${THREAT_ID}). File ${QUARANTINED}. File was repaired.
6. Customize the notification for file infected message.

Command:

```
xmldiffuser -s
//policies/ThreatPolicies/Notifications/FileInfectedNotificationText/@value
<text> policy.xml
```

Default value: File: $\{FILE\_NAME\} was infected with $\{THREAT\_NAME\}$ ($\{THREAT\_ID\}$). File $\{QUARANTINED\}$. File is still infected.

7. Customize the notification for the total number of viruses found message.

Command:

```
xmldiffuser -s
//policies/ThreatPolicies/Notifications/TotalVirusFoundNotificationText/@value
<text> policy.xml
```

Default value: This email message was infected. $\{TOTAL\_THREATS\}$ number of viruses were found.

8. Customize the notification for the denied file size message.

Command:

```
xmldiffuser -s
//filtering/FileAttribute/DenyFileSizesNotificationText/@value
<text> filtering.xml
```

Default value: The file attached to this email was removed because the file size is not allowed. File attachment: $\{FILE\_NAME\}$. Matched file size: $\{FILE\_SIZE\}$.

9. Customize the notification for the denied file names message.

Command:

```
xmldiffuser -s
//filtering/FileAttribute/DenyFileNamesNotificationText/@value
<text> filtering.xml
```

Default value: The file attached to this email was removed because the file name is not allowed. File attachment: $\{FILE\_NAME\}$. Matched pattern: $\{MATCHING\_FILENAME\_ENTRY\}$. 
10 Customize the notification for the denied encrypted container message.

**Command:**
```
xmmodiﬁer -s //ﬁltering/Container/EncryptedContainersHandling/NotificationText/@value <text> ﬁltering.xml
```

**Default value:** The encrypted container attached to this email was removed. File attachment: ${FILE_NAME}. File ${QUARANTINED}.

11 Customize the notification for the denied malformed container message.

**Command:**
```
xmmodiﬁer -s //ﬁltering/Container/MalformedContainersHandling/NotificationText/@value <text> ﬁltering.xml
```

**Default value:** The malformed container attached to this email was removed. File attachment: ${FILE_NAME}. File ${QUARANTINED}.

12 Customize the notification for the APK violation message.

```
xmmodiﬁer -s //policies/ThreatPolicies/Notifications/APKFileDeletedNotificationText/@value <text> policy.xml
```

**Default value:** File: ${FILE_NAME} violates APK reputation policy. File ${QUARANTINED}. File was deleted.

13 Restart the Symantec Protection Engine service.

**Notifying RPC client users that a threat was found in the Core server only mode**

If your client uses RPC, you can configure Symantec Protection Engine to notify a user that a file cannot be retrieved from an RPC Network Attached Storage client because it contains a threat.

The notification message includes the following information:

- Date and time of the event
- Name of the infected file
- Threat name and ID
- Manner in which the infected file was handled (for example, whether the file was repaired or deleted)
The notification message also includes information about the Symantec Protection Engine that detected the infection. For example, the message contains the IP address and the port number of Symantec Protection Engine. The message also contains the date and the revision number of the definitions that were used to detect the threat.

This feature is only available on Windows. The requesting user's computer must be in the same domain as Symantec Protection Engine. The Windows Messenger service must be running both on the computer on which Symantec Protection Engine is running and on the user's computer. If the notification information cannot be delivered to the requesting user, a failure message is logged.

To notify RPC client users that a threat was found

1. Go to the Symantec Protection Engine installation directory.
2. Notify RPC client users.
   
   **Command:**
   
   `xmlmodifier -s //configuration/Logging/LogPopup/@value true configuration.xml`
   
   **Allowed values:**
   
   - true
     
     Notifies the RPC client users that a threat was found.
   - false
     
     Does not notify the RPC client users that a threat was found.
   
   **Default value:** false
3. Restart the Symantec Protection Engine service.

See “About scanning for risks” on page 110.

Enabling Symantec Insight™ in the Core server only mode

Insight scanning is enabled by default. You must have a valid Insight scanning license to scan for threats and to update Insight feeds.

Symantec Protection Engine also gives you an option to quarantine threats. You can quarantine threats if you have configured the Quarantine server in Symantec Protection Engine.
Note: If Insight is enabled then all main categories (including security risks, advanced heuristics) are enabled by default in Symantec Protection Engine irrespective of whether Security Risks and Advanced heuristics scanning policy for Antivirus scanning is disabled or enabled.

To enable Symantec Insight™ in Symantec Protection Engine

1. Go to the Symantec Protection Engine installation directory.

2. Enable reputation-based Insight protection.
   
   **Command:**
   
   `xmlmodifier -s //policies/ThreatPolicies/InsightScanning/@enabled true policy.xml`
   
   **Allowed values:**
   
   - true
     
     Enables the Symantec Insight feature.
   
   - false
     
     Disables the Symantec Insight feature.
   
   **Default value:** true

3. Specify how Symantec Protection Engine should handle the files detected by Symantec Insight.
   
   **Command:**
   
   `xmlmodifier -s //policies/ThreatPolicies/Actions/InsightActionPolicy/@value <value> policy.xml`
   
   **Allowed values:**
   
   - 0
     
     Log only: Generates a log entry for the files that are detected by Symantec Insight.
   
   - 1
     
     Block: Blocks the files that are detected by Symantec Insight and generates a log entry.
   
   - 2
     
     Delete: Deletes the files that are detected by Symantec Insight and generates a log entry.
   
   **Default value:** 2

4. Restart the Symantec Protection Engine service.
Configuring the Symantec Insight™ aggression level in the Core server only mode

The Insight Aggression Level defines how sensitive the Insight feature is to a file's reputation score. Higher the aggression level, more are the number of files that are detected as threats. However, there is a possibility of false positives.

To enable the Insight aggression level

1. Go to the Symantec Protection Engine installation directory.
2. Specify the aggression level for Symantec Insight.

Command:

```
xmlmodifier -s
//policies/ThreatPolicies/InsightScanning/InsightPolicy/AggressionLevel/@value
<value> policy.xml
```

**Allowed values:**

- 1
  
  Low

- 2
  
  Medium

- 3
  
  High

**Note:** The Insight aggression level defines how sensitive the Symantec Insight feature is to a file's reputation score.

**Default value:** 2

3. Restart the Symantec Protection Engine service.

See “To configure Symantec Insight™ policy” on page 141.

Excluding files from Insight scanning based on file size in the Core server only mode

You can enter a file size criteria to exclude files from scanning.
To exclude files based on file size

1. Go to the Symantec Protection Engine installation directory.
2. Specify the file size (in bytes), above which Insight excludes the file from scanning.
   
   **Command:**
   ```
   xmlmodifier -s
   //policies/ThreatPolicies/InsightScanning/InsightPolicy/FileSizeExclusionThreshold/@value
   <value> policy.xml
   ```

   **Allowed values:**
   - Type the file size in bytes.
   - Minimum value is 1 and maximum value is 2147000000.

   **Default value:** 134217728 (bytes)

3. Restart the Symantec Protection Engine service.

   See “To configure Symantec Insight™ policy” on page 141.

Excluding files from Insight scanning based on SHA256 in the Core server only mode

You can enter the SHA256 value of files that you want to exclude from scanning.

**Note:** Only 500 entries are allowed. Any entry above 500 is removed automatically.

To exclude files based on SHA256

1. Go to the Symantec Protection Engine installation directory.
2. Create a text file and type the SHA256 values of the files to exclude from Insight scanning. The values of the files to be excluded should be one line per entry.
   
   **Command:**
   ```
   xmlmodifier -b
   //policies/ThreatPolicies/InsightScanning/InsightPolicy/SHA256ExclusionList/items
   <file name> policy.xml
   ```

   **For example,** `xmlmodifier -b
   //policies/ThreatPolicies/InsightScanning/InsightPolicy/SHA256ExclusionList/items
   Sample.txt policy.xml`

   **Allowed values:**
Excluding files from Insight scanning based on source IP address in the Core server only mode

You can configure Insight scanning to exclude files based on source IPs.

To exclude files based on based on source IP

1. Go to the Symantec Protection Engine installation directory.
2. Create a text file and type the source IPs of the files to exclude from Insight scanning. Source IPs of the files to exclude from insight scanning should be entered one line per entry.

Command:

```
xmmodifier -b
//policies/ThreatPolicies/InsightScanning/InsightPolicy/SourceIPExclusionList/items
<file name> policy.xml
```

For example, `xmlmodifier -b
//policies/ThreatPolicies/InsightScanning/InsightPolicy/SourceIPExclusionList/items
SampleSourceIPs.txt policy.xml`

Allowed values:

- Allowed values are valid IPv4/IPv6 addresses.
- Maximum allowed entries for this list are 500 and minimum 0.

3. Restart the Symantec Protection Engine service.

See “To configure Symantec Insight™ policy” on page 141.

Excluding files from Insight scanning based on source URL in the Core server only mode

You can configure Insight scanning to exclude files based on source URLs.
To exclude files based on source URL

1. Go to the Symantec Protection Engine installation directory.
2. Create a text file and type the source URLs of the files to exclude from Insight scanning. The source URLs of the files to exclude from Insight scanning should be entered one line per entry.

Command:

```
xmlmodifier -b
//policies/ThreatPolicies/InsightScanning/InsightPolicy/SourceURLExclusionList/items
<file name> policy.xml
```

For example, `xmlmodifier -b
//policies/ThreatPolicies/InsightScanning/InsightPolicy/SourceURLExclusionList/items` SampleSourceURLs.txt policy.xml

**Allowed values:**

- Allowed values are valid URLs.
- Maximum allowed entries for this list are 500 and minimum 0.

3. Restart the Symantec Protection Engine service.

See “To configure Symantec Insight™ policy” on page 141.

Monitoring scanning requests in the Core server only mode

Symantec Protection Engine provides a feature that lets you define the expected scanning load for specific time periods. When the Symantec Protection Engine scanning load decreases significantly, it might indicate a performance issue. You can use this feature to detect possible problems before they become critical. If Symantec Protection Engine detects fewer scan requests than the expected load, it logs the event to the designated logging destinations and alert destinations. The event is logged at the Warning level.

See “Logging levels and events” on page 202.

Symantec Protection Engine averages the number of scan requests for one minute. If the average number of requests for that minute meets or exceeds the threshold, no alert is sent. If the average number of scan requests for that minute is below the threshold, Symantec Protection Engine sends an alert.

For example, if you set a threshold of 20 requests per second for Wednesday from 1:00 A.M. to 2:00 A.M., Symantec Protection Engine does not generate an alert for any minute in which it receives 1,200 or more requests (20 requests times 60
seconds). Symantec Protection Engine only generates an alert for any minute in which it receives fewer than 1,200 requests.

You can control how scanning requests are monitored by editing the Configuration.xml file. Add an entry in the Configuration.xml file in the following format:

```xml
<Weekday>
  <Schedule enable="true" start="<start time in 24-hour format>"
  end="end time in 24-hour format" threshold="<requests per second>"/>
</Weekday>
```

You can control how scanning requests are monitored in the following ways:

- Enable or disable the scan request monitor feature.
- Add a new schedule.
- Activate or deactivate an existing schedule.
- Delete a schedule.

To enable or disable the scan request monitor feature

1. Go to the Symantec Protection Engine installation directory and edit the Configuration.xml file.

2. Configure monitoring of scanning requests.

   Command:

   ```bash
   xmlmodifier -s //configuration/Miscellaneous/RequestMonitoringSchedules/
   EnableRequestMonitoring/@value true configuration.xml
   ```

   **Allowed values:**

   - true
     Enables monitoring scanning requests in Symantec Protection Engine.
   - false
     Disables monitoring scanning requests in Symantec Protection Engine.

   **Default value:** false

3. Restart the Symantec Protection Engine service.
To add a new schedule

1. Go to the Symantec Protection Engine installation directory and edit the Configuration.xml file.

2. Add the following tags:

```
<Weekday>
  <Schedule enable="true" start="<start time in 24-hour format>" end="<end time in 24-hour format>" threshold="<requests per second>"/>
</Weekday>
```

For example:

```
<RequestMonitoringSchedules>
  <EnableRequestMonitoring value="true"/>
  <ExistingSchedules>
    <Tuesday>
      <Schedule enable="true" start="23" end="0" threshold="10"/>
    </Tuesday>
  </ExistingSchedules>
</RequestMonitoringSchedules>
```

3. Restart the Symantec Protection Engine service.

To activate or deactivate an existing schedule

1. Go to the Symantec Protection Engine installation directory and edit the Configuration.xml file.

2. Edit the value in the following tag:

```
<Schedule enable="<value>" start="23" end="0" threshold="10"/>
```

**Allowed values:**

- **true**
  - Activate an existing schedule.
- **false**
  - Deactivate an existing schedule.

3. Restart the Symantec Protection Engine service.
To delete a schedule

1  Go to the Symantec Protection Engine installation directory and edit the Configuration.xml file.
2  Delete the following tag:

   <Schedule enable="<value>" start="23" end="0" threshold="10"/>

3  Restart the Symantec Protection Engine service.

See "How to monitor Symantec Protection Engine performance" on page 145.

Enabling resource consumption logging in the Core server only mode

Symantec Protection Engine captures the resources data every 5 seconds and logs it every one minute. Thus, every minute 12 rows are added to the log file. The resource consumption log files are saved in the default log directory as .rcl files.

To enable resource consumption logging in Symantec Protection Engine

1  Go to the Symantec Protection Engine installation directory.
2  Enable resource consumption logging.

   Command:

   xmlmodifier -s //configuration/Logging/LogResourceInfo/@enabled true configuration.xml

   Allowed values:

   ■  true
       Enables resource consumption logging in Symantec Protection Engine.
   ■  false
       Disables resource consumption logging in Symantec Protection Engine.

   Default value: true

3  Specify the number of individual log files to retain (one per day).

   Command:

   xmlmodifier -s //configuration/Logging/LogResourceInfo/@logfilestokeep <value> configuration.xml

   Allowed values:
Specifying the maximum file or message size to scan in the Core server only mode

If your client uses the ICAP protocol, you can specify a maximum size of files or messages to scan. For messages, the maximum size includes the size of the entire message body and all attachments. For container files, the maximum size includes the container file and all of its contents. The files and mail messages that meet or exceed the maximum file size are blocked.

By default, Symantec Protection Engine has no limits on total file or message sizes.

To specify the maximum file or message size to scan

1. Go to the Symantec Protection Engine installation directory.
2. Specify the maximum file size (in bytes) that Symantec Protection Engine should accept.
   
   **Command:**
   ```
   xmlmodifier -s //filtering/FileAttribute/FileSizeScanThreshold/@value <value> filtering.xml
   ```
   
   **Allowed values:**
   
   - 1 to 2147483648 (2 GB)
   - 0
     
     This setting places no limits on file or message size but internal component can handle up to 2 GB at most.
     
     **Default value:** 0 (bytes)
   
3. Restart the Symantec Protection Engine service.

See “Enhance performance by limiting scanning” on page 156.
Setting container file limits in the Core server only mode

Symantec Protection Engine protects your network from the file attachments that can overload the system and consume scanning performance and degrade performance.

This protection includes the container files that have any of the following characteristics:

- Overly large.
- Contain large numbers of embedded, compressed files.
- Are designed to maliciously use resources and degrade performance.

To enhance scanning performance and reduce your exposure to denial-of-service attacks, you can impose limits to control how Symantec Protection Engine handles container files.

You can specify the following limits for handling container files:

- The maximum amount of time, in seconds, that is spent decomposing a container file and its contents. This setting does not apply to .hqx or .amg files.
- The maximum file size, in MB, for the individual files that are in a container file.
- The maximum number of nested levels to be decomposed for scanning.
- The maximum number of bytes that are read when determining whether a file is MIME-encoded.

Symantec Protection Engine scans a file and its contents until it reaches the maximum depth that you specify. Symantec Protection Engine stops scanning any file that meets the maximum file size limit or that exceeds the maximum amount of time to decompose. It then generates a log entry. Symantec Protection Engine resumes scanning any remaining files. This process continues until Symantec Protection Engine scans all of the files to the maximum depth (that do not meet any of the processing limits).

You can specify whether to allow or to deny access to files for which an established limit is met or exceeded. Access is denied by default.

**Warning:** If you allow access to a file that has not been fully scanned, you can expose your network to risks. If you allow access and Symantec Protection Engine detects a risk, it does not repair the file, even if under normal circumstances the file can be repaired. In this case, the file is handled as though the file is unrepairable.
To set container file limits

1. Go to the Symantec Protection Engine installation directory.
2. Specify the maximum time that Symantec Protection Engine can spend extracting a single container file.
   
   **Command:**
   ```
   xmlmodifier -s //filtering/Container/MaxExtractTime/@value <value>
   filtering.xml
   ```
   
   **Allowed values:**
   - 1 to 86400 (seconds)
   - 0
     
     Disables this setting (so that no limit is imposed).
   
   **Default value:** 180 (seconds)

3. Specify the maximum file size, in MB, for individual files in a container file.
   
   **Command:**
   ```
   xmlmodifier -s //filtering/Container/MaxExtractSize/@value <value>
   filtering.xml
   ```
   
   **Allowed values:**
   - 1 to 30719 (MB)
     
     The maximum value that you can specify for individual files in tar, rar, and zip containers is 30719 MB (~30 GB). The maximum value that you can specify for other containers is 1907 MB (~2 GB).
   
   - 0
     
     Disables this setting (so that no limit is imposed).
   
   **Default value:** 100 (MB)

4. Specify the maximum depth of the container file that Symantec Protection Engine can extract for scanning.
   
   **Command:**
   ```
   xmlmodifier -s //filtering/Container/MaxExtractDepth/@value <value>
   filtering.xml
   ```
   
   **Allowed values:**
   - 1 to 50
   
   **Default value:** 10
5 Specify the maximum number of files that Symantec Protection Engine can extract for scanning.

**Command:**

```
xmlmodifier -s //filtering/Container/MaxExtractFileCount/@value <value> filtering.xml
```

**Allowed values:**

- 0 to 32212254720

**Default value:** 0

6 Specify the action for the container files that exceed the limit for extract depth, time, size, file count, and maximum cumulative extract size.

**Command:**

```
xmlmodifier -s //filtering/Container/<MaxExtractDepth, MaxExtractTime, MaxExtractSize, MaxExtractFileCount, or MaxCumulativeExtractSize>/@actionpolicy <value> filtering.xml
```

**Allowed values:**

- 0
  - Creates a log entry and allows access to the file.
- 1
  - Blocks access to the file.

For example,

To block the access to the container file that exceeds the limit for max extract file size, run the following command:

```
xmlmodifier -s //filtering/Container/MaxExtractSize/@actionpolicy<value> filtering.xml
```

7 Specify the maximum number of bytes that Symantec Protection Engine should scan to determine whether a file is MIME-encoded.

**Command:**

```
xmlmodifier -s //filtering/Container/Options/NonMIMEThreshold/@value <value> filtering.xml
```

**Allowed values:**

- 0 to 200000
Default value: 200000 (bytes)

8 Restart the Symantec Protection Engine service.

See “Enhance performance by limiting scanning” on page 156.

Enabling URL filtering in the Core server only mode

Symantec Protection Engine is provided with minimum URL definitions. We recommend you to run LiveUpdate and update the URL definitions before you start URL filtering.

URL filtering can be enabled during installation. If you did not enable URL filtering during installation, follow the steps below to enable it.

To enable URL filtering in Symantec Protection Engine

1 Go to the Symantec Protection Engine installation directory.

2 Enable URL filtering.

Command:

```
xmlmodifier -s //filtering/URLFilter/@enabled true filtering.xml
```

Allowed values:

- **true**
  - Enables URL filtering.

- **false**
  - Disables URL filtering.

Default value: false

3 Select the Filtering mode or Audit mode.

Command:

```
xmlmodifier -s //filtering/URLFilter/FilteringMode/@value <value>
```

filtering.xml

Allowed values:

- **1**
  - Filtering mode

- **0**
  - Audit mode

Default value: 1

4 Restart the Symantec Protection Engine service.
Denying access to URLs in URL categories in the Core server only mode

Symantec Protection Engine includes predefined URL categories. URL categories consist of URLs that contain related subject matter. You can deny access to URLs when you add the category to the DenyVendorCategories list. When you deny access to a URL category, access to the URLs that are contained in that category is denied. However, you can override the categorization of a URL.

See “Overriding a URL categorization” on page 189.

None of the URL categories are in the DenyVendorCategories list and access to the URLs in every category is permitted by default. You must select the URL categories that you want to add to the DenyVendorCategories list.

To deny access to URLs in URL categories

1. Go to the Symantec Protection Engine installation directory.
2. Add URL categories that you want to block.
   
   Create a text file and add the URL categories, which you want to block. These categories are case sensitive.

   **Command:**
   
   `xmlmodifier -b //filtering/URLFilter/DenyVendorCategories/items <name of the text file created above> filtering.xml`

   **Allowed categories:** Valid vendor categories to be blocked

   See “About predefined URL categories” on page 168.
3. Restart the Symantec Protection Engine service.

Customizing the access denied message in the Core server only mode

Symantec Protection Engine displays an Access denied message to the user when access to a Web site is blocked. The default message is as follows:

Access to the destination `${URL_REQUESTED}` is prohibited. `${REASON}`

You can customize the message using the following variables:

`${URL_REQUESTED}` The URL address that the user requested.
An explanation of why the URL address that the user requests is blocked.

When a Web site is blocked due to URL violation, the ${REASON} variable reads as follows:

Found in denied list <(category)>

where <(category)> is the URL or local category that contains the URL that is denied.

To customize the access denied message

1. Go to the Symantec Protection Engine installation directory.
2. Customize the access denied message.

   Command:

   xmlmodifier -s //filtering/URLFilter/AccessDeniedMessage/@value
   <customize the user notification message> filtering.xml

   Default value: Access to the destination ${URL_REQUESTED} is prohibited. ${REASON}

3. Restart the Symantec Protection Engine service.

See “How to filter a URL” on page 182.

Specifying the log bind address in the Core server only mode

You can set a log bind address for each Symantec Protection Engine so that you can more easily identify the originating protection engine. When you use this feature, the log bind address of the originating Symantec Protection Engine is included in all alert messages.

For example, setting the log bind address is helpful if you have multiple Symantec Protection Engines that listen on the loopback interface (127.0.0.1). The IP address on which Symantec Protection Engine listens is used in SNMP and SMTP alert messages to identify the originating Symantec Protection Engine. Therefore, it is not possible to determine which Symantec Protection Engine originated the message when more than one uses the loopback interface. You can set a unique log bind address for each Symantec Protection Engine to provide a method for identifying each Symantec Protection Engine.

If your client uses ICAP and you do not specify a log bind address, Symantec Protection Engine selects one for you. Symantec Protection Engine determines the log bind address based on the scanning bind addresses.
To specify the log bind address in Symantec Protection Engine

1. Go to the Symantec Protection Engine installation directory.
2. In the Log bind address parameter, type an IP address to identify the computer on which Symantec Protection Engine is running.

   **Command:**

   ```bash
   xmlmodifier -s //configuration/ProtocolSettings/ICAP/BindAddress/@value <value> configuration.xml
   ``

   **Allowed values:** Valid IP address
3. Restart the Symantec Protection Engine service.

   See “Configuring ICAP options” on page 98.

Specifying the local logging level in the Core server only mode

Symantec Protection Engine sends logging events to the local logs by default. You can change the types of events that are sent to the local logs. The default logging level for the local logs is Warning.

See “Changing the directory where log files are located” on page 208.

To specify the local logging level

1. Go to the Symantec Protection Engine installation directory.
2. Specify the local logging level.

   **Command:**

   ```bash
   xmlmodifier -s //configuration/Logging/LogLocal/@loglevel <value> configuration.xml
   ``

   **Allowed values:**

   - 0
     None
   - 1
     Error
   - 2
     Outbreak
   - 3
     Warning
4 Information
5 Verbose
6 Audit

Default value: 3

The default logging level is Warning. Select Verbose only if you have been instructed to do so by Symantec Technical Support to troubleshoot issues.

Restart the Symantec Protection Engine service.

Changing the directory where log files are located in the Core server only mode

You can change the location of the local log file and the statistics log files. You cannot change the file names. The default location for the log files for Linux is opt/SYMC Scan/log. The default location for Windows platform is C:\Program Files\Symantec\Scan Engine\log.

Symantec Protection Engine creates a new local log file for each day. The file names have the following format: SSEyyyymmdd.log, where yyyy is the year, mm is the month, and dd is the day.

The disk space that is required for the log files varies, depending upon your scan volume, associated activity, and how long you retain the log files. The specified location must be large enough to accommodate these files. If you change the log file location, old log files remain in the former directory and are not removed during uninstallation. Old logs must be removed manually.
To change the directory where log files are located

1. Go to the Symantec Protection Engine installation directory.

2. Change the directory where log files are located.

   **Command:**
   
   ```
   xmlmodifier -s //configuration/Logging/LogDir/@value "valid log directory" configuration.xml
   ```

   **Allowed values:** Valid directory path.

   **Default value:** Symantec Protection Engine installation directory.

   **Windows:** C:\Program Files\Symantec\Scan Engine\log
   
   **Linux:** /opt/symcscan/log

3. Restart the Symantec Protection Engine service.

See “Changing the length of time that log files are maintained” on page 210.

## Maintaining log files on a shared resource in Windows in the Core server only mode

You can store the Symantec Protection Engine log files on a shared resource. Make sure that the shared resource has adequate disk space. To optimize security, you should restrict full access rights on the shared resource to the administrator user of the host on which Symantec Protection Engine is installed.

**Note:** To enhance Symantec Protection Engine performance, maintain the log files locally instead of writing log data to a remote, shared resource.

Before you perform the following procedure, ensure that you are an administrator of the host on which Symantec Protection Engine is installed. Also ensure that you have full permissions on the shared resource.

**To maintain log files on a shared resource in Windows**

1. Map or mount the shared resource from the host on which Symantec Protection Engine is installed.

   For more information about how to map or mount a shared resource, see the documentation for your operating system.

2. Stop the Symantec Protection Engine service.

3. Change the account of the Symantec Protection Engine service to the Administrator.
Changing the number of log file to be maintained in the Core server only mode

Symantec Protection Engine creates a new log file for each day. You can specify the number of log files that Symantec Protection Engine retains to keep the log directory at a manageable size. Thus, when the maximum number of log files is reached, the oldest log file is removed on a daily basis. In its default configuration, this setting is enabled and the default value is 0. That means all the log files are retained.

To change the length of time for which the log files are maintained

1  Go to the Symantec Protection Engine installation directory.
2  Specify the number of log files that you want to maintain.
   Command:
   xmlmodifier -s //configuration/Logging/LogLocal/@logfilestokeep <value> configuration.xml
   Allowed values: 0 to 365
   Default value: 0
3  Restart the Symantec Protection Engine service.
See “Exporting local log data to a file” on page 220.
Enabling statistics reporting in the Core server only mode

You can configure Symantec Protection Engine to maintain and report cumulative scan data. You must enable logging to the statistics logs so that you can view statistics reports. You can select a date range and time range for the report and view the scanning statistics for that range.

See “Viewing statistics log data” on page 221.

Symantec Protection Engine creates a new statistics log file for each day. The file name has the following format: SSEyyyymmdd.dat, where yyyy is the year, mm is the month, and dd is the day.

The statistics log files are stored in the same location as the log files. The default location for the log files for Linux is /opt/SYMCScan/log. The default location for Windows is C:\Program Files\Symantec\Scan Engine\log.

To enable statistics reporting in Symantec Protection Engine

1. Go to the Symantec Protection Engine installation directory.
2. Enable statistics reporting in Symantec Protection Engine.
   
   **Command:**

   ```bash
   xmlmodifier -s //configuration/Logging/LogStatistics/@enabled <true> configuration.xml
   ```

   **Allowed values:**

   - true
     Enables statistics reporting in Symantec Protection Engine.
   - false
     Disables statistics reporting in Symantec Protection Engine.

   **Default value:** true

3. Restart the Symantec Protection Engine service.

See “Changing the length of time that log files are maintained” on page 210.

See “About configuring local logging” on page 207.
Configuring logging to the Windows Application Event Log in the Core server only mode

If you are running Symantec Protection Engine on Windows, you can configure Symantec Protection Engine to log events to the Windows Application Event Log. You can also select the types of events that are logged. The default logging level is None (deactivated).

To configuring logging to the Windows Application Event Log

1. Go to the Symantec Protection Engine installation directory.
2. Configure logging to the Windows Application Event Log.
   
   **Command:**
   
   `xmlmodifier -s //configuration/Logging/LogWindows/@loglevel configuration.xml`

   **Allowed values:**
   
   - 0
     None
   - 1
     Error
   - 2
     Outbreak
   - 3
     Warning
   - 4
     Information
   - 5
     Verbose
   - 6
     Audit

   **Default value:** 0

3. Restart the Symantec Protection Engine service.

See “Logging levels and events” on page 202.
Configuring logging to the Linux Syslog in the Core server only mode

If you are running Symantec Protection Engine on Linux, you can configure Symantec Protection Engine to log events to the Linux Syslog. You can also select the types of events that are logged. The default logging level is None (deactivated). Logs are saved at /var/log/messages location.

You must be running Symantec Protection Engine on Linux to use this feature.

To configure logging to the Linux Syslog

1. Go to the Symantec Protection Engine installation directory.
2. Configure logging to the Linux Syslog.

   Command:

   ```sh
gxmlmodifier -s //configuration/Logging/Syslog/@loglevel <value> configuration.xml
```

   Allowed values:

   - 0
     None
   - 1
     Error
   - 2
     Outbreak
   - 3
     Warning
   - 4
     Information
   - 5
     Verbose
   - 6
     Audit

3. Restart the Symantec Protection Engine service.

Activating SMTP alerts in the Core server only mode

When you activate SMTP alerts, you must identify a primary SMTP server for forwarding alert messages. You must also specify the email addresses of the
recipients and the local domain for Symantec Protection Engine. You can specify a second SMTP server if one is available.

You must select the types of events for which SMTP alert messages are generated.

**To activate SMTP alerts**

1. Go to the Symantec Protection Engine installation directory.
2. Configure the SMTP notification level.
   
   **Command:**
   
   ```
   xmlmodifier -s //configuration/Logging/LogSMTP/@loglevel <value>
   configuration.xml
   ```
   
   **Allowed values:**
   
   - 0
     None
   - 1
     Error
   - 2
     Outbreak
   - 3
     Warning
   - 4
     Information
   - 6
     Audit

   **Default value:** 0
   
   SMTP alerts are not activated by default. The SMTP notification level is set to None. The Verbose notification level is not available for SMTP alerting.

3. In the Primary server address parameter, configure the IP address or host name of the primary SMTP server that forwards the alert messages.

   **Command:**
   
   ```
   xmlmodifier -s //configuration/Logging/LogSMTP/@primary <value>
   configuration.xml
   ```
   
   **Allowed values:** Valid IP address or the host name of the SMTP server.
4 In the secondary server address parameter, type the IP address or host name of a secondary SMTP server (if one is available) that forwards the alert messages if communication with the primary SMTP server fails.

Command:

```
xmlmodifier -s //configuration/Logging/LogSMTP/@secondary <value> configuration.xml
```

**Allowed values:** Valid IP address or the host name of the SMTP server.

5 In the SMTP domain parameter, type the local domain for Symantec Protection Engine.

Command:

```
xmlmodifier -s //configuration/Logging/LogSMTP/@domain <domain name> configuration.xml
```

The domain name is added to the "From" box for SMTP messages. SMTP alert messages that Symantec Protection Engine generates originate from SymantecProtectionEngine@<domainname>, where <domainname> is the domain name that you specify in the SMTP domain parameter.

6 Create a text file and add the email addresses of the recipients of the SMTP alert messages. You can add multiple email address in the same file. Ensure you type one entry per line.

Command:

```
xmlmodifier -b //configuration/Logging/LogSMTP/RecipientList/items <name of the text file created above> configuration.xml
```

7 Restart the Symantec Protection Engine service.

See “Logging levels and events” on page 202.

See “About configuring alerts” on page 213.

---

**Activating SNMP alerts in the Core server only mode**

To activate SNMP alerts, you must provide the SNMP community string and an IP address for a primary SNMP console for receiving the alert messages. You can specify a second SNMP console if one is available. A secondary SNMP console is optional. Alert messages are sent to the primary SNMP console and secondary SNMP console in all instances. You can also configure ports for the primary server and secondary server.

The Management Information Base file (symantecprotectionengine.mib) is located in the Tools\MIB folder in the
Symantec_Protection_Engine_Tools_7.8.0.XX_IN.zip file. You can use the symantecprotectionengine.mib file to configure the SNMP alerts.

You must select the types of events for which SNMP alert messages are generated.

To activate SNMP alerts

1. Go to the Symantec Protection Engine installation directory.
2. Configure the SNMP notification level.
   
   **Command:**
   ```
   xmlmodifier -s //configuration/Logging/LogSNMP/@loglevel <value> configuration.xml
   ```

   **Allowed values:**
   - 0
     None
   - 1
     Error
   - 2
     Outbreak
   - 3
     Warning
   - 4
     Information
   - 6
     Audit

   **Default value:** 0

   SNMP alerts are not activated by default. The SNMP notification level is set to None. The Verbose notification level is not available for SNMP alerting.

3. In the Primary server address parameter, configure the IP address or host name of the primary SNMP server that forwards the alert messages.

   **Command:**
   ```
   xmlmodifier -s //configuration/Logging/LogSNMP/@primary <value> configuration.xml
   ```

   **Allowed values:** Valid IP address or the host name of the SNMP server.
4 In the Primary server port parameter, type the port number of the primary SNMP console to receive the alert messages.

   Command:
   
   xmlmodifier -s //configuration/Logging/LogSNMP/@primaryport <value> configuration.xml

   Allowed values: Valid port number of the primary SNMP console to receive the alert messages.

   Default value: 162

5 In the secondary server address parameter, type the IP address or host name of a secondary SNMP server (if one is available) that forwards the alert messages if communication with the primary SNMP server fails.

   Command:
   
   xmlmodifier -s //configuration/Logging/LogSNMP/@secondary <value> configuration.xml

   Allowed values: Valid IP address or the host name of the SNMP server.

6 In the secondary server port parameter, type the port number of the primary SNMP console to receive the alert messages.

   Command:
   
   xmlmodifier -s //configuration/Logging/LogSNMP/@secondaryport/<value> configuration.xml

   Allowed values: Valid port number of the secondary SNMP console to receive the alert messages.

   Default value: 162

7 Restart the Symantec Protection Engine service.

   See "Logging levels and events" on page 202.

   See “About configuring alerts” on page 213.

Configuring outbreak alerts in the Core server only mode

Symantec Protection Engine can issue alerts when a specified number of the same type of threat or policy violation occurs in a given time interval. You can use outbreak alerts as an early warning for potential outbreaks. Alerts of outbreaks can help you take the necessary precautions to protect your network.
You can select the types of events for which you want to receive alerts. For each event type, you can configure the threshold number of occurrences and the time interval. If the number of occurrences meets or exceeds the configured threshold for the selected interval, Symantec Protection Engine generates an alert.

Table 12-8 lists the outbreak alert events that you can configure.

### Table 12-8 Outbreak alert events

<table>
<thead>
<tr>
<th>Event</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virus</td>
<td>A viral threat was detected.</td>
</tr>
<tr>
<td>Infection</td>
<td>An infection was detected.</td>
</tr>
<tr>
<td>MailPolicy</td>
<td>A mail policy violation occurred.</td>
</tr>
<tr>
<td>urlblock</td>
<td>A URL was blocked due to a URL filtering violation.</td>
</tr>
<tr>
<td>ContainerLimit</td>
<td>A maximum file extraction time/size/depth was met or exceeded.</td>
</tr>
<tr>
<td>MalformedContainer</td>
<td>A malformed container was detected and blocked.</td>
</tr>
<tr>
<td>FileAttribute</td>
<td>Any file attribute violation was detected.</td>
</tr>
<tr>
<td>AnyNonViral</td>
<td>A nonviral threat was detected.</td>
</tr>
<tr>
<td>SameNonViral</td>
<td>One or more incidence of the same type of nonviral threat was detected.</td>
</tr>
<tr>
<td>HighRisk</td>
<td>A high risk rating threat was detected.</td>
</tr>
<tr>
<td>MediumRisk</td>
<td>A medium risk rating threat was detected.</td>
</tr>
<tr>
<td>InsightDetected</td>
<td>A threat was detected by Insight.</td>
</tr>
</tbody>
</table>

### To configure outbreak alerts

1. Go to the Symantec Protection Engine installation directory.
2. Enable outbreak for a threat or policy violation event.

   Command:
   ```
   xmlmodifier -s //configuration/Logging/Outbreak/<Threat or Policy Violation Event>/@enabled true configuration.xml
   ```
   
   Where, threat or policy violation event can be **Infection**, **Virus**, **MalformedContainer**, **MailPolicy**, **ContainerLimit**, **FileAttribute**, **urlblock**, **AnyNonViral**, **SameNonViral**, **HighRisk**, **MediumRisk**, and **InsightDetected**.

   For example, to enable an outbreak alert for any malformed container violation,
xmlmodifier -s
//configuration/Logging/Outbreak/MalformedContainer/@enabled true
configuration.xml

**Allowed values:**

- **true**
  - Enables an outbreak alert.

- **false**
  - Disables an outbreak alert.

**Default value:** false

3 Configure time interval for an outbreak alert.

This parameter configures time interval. If number of threats or policy violations detected are more than the configured threshold value in this time interval, Symantec Protection Engine generates an outbreak alert.

**Command:**

```bash
xmlmodifier -s //configuration/Logging/Outbreak/<Threat or Policy Violation Event>/@interval<interval in seconds> configuration.xml
```

Where, threat or policy violation event can be Infection, Virus, MalformedContainer, MailPolicy, ContainerLimit, FileAttribute, urlblock, AnyNonViral, SameNonViral, HighRisk, MediumRisk, and InsightDetected.

For example, to configure the time interval for any malformed container violation,

```bash
xmlmodifier -s //configuration/Logging/Outbreak/MalformedContainer/@interval 300 configuration.xml
```

**Allowed values:** 1 to 1000000 seconds

**Default value:** 1 second
4 Configure the threshold value for an outbreak alert.

This parameter configures a threshold value for a threat or policy violation. If those threat or policy violations detected are more than the configured threshold value in the configured time interval, Symantec Protection Engine generates an outbreak alert.

Command:

```
xmlmodifier -s //configuration/Logging/Outbreak/<Threat or Policy Violation Event>/@threshold <threshold value> configuration.xml
```

Where, threat or policy violation event can be Infection, Virus, MalformedContainer, MailPolicy, ContainerLimit, FileAttribute, urlblock, AnyNonViral, SameNonViral, HighRisk, MediumRisk, and InsightDetected.

For example, to configure the threshold value for any malformed container violation,

```
xmlmodifier -s //configuration/Logging/Outbreak/MalformedContainer/@threshold 10 configuration.xml
```

**Allowed values:** 2 to 1000000

**Default value:** 2

5 Restart the Symantec Protection Engine service.

See “About configuring alerts” on page 213.

See “Logging levels and events” on page 202.

---

**Configuring LiveUpdate to occur automatically in the Core server only mode**

You can schedule LiveUpdate to occur automatically at a specified time interval to ensure that Symantec Protection Engine always has the most current definitions. When you install a valid antivirus content license or URL content license, Symantec Protection Engine automatically tries to perform a LiveUpdate. By default, Symantec Protection Engine is configured to perform a LiveUpdate every two hours.

When LiveUpdate is scheduled, it runs at the specified time interval that is relative to the LiveUpdate base time. The default LiveUpdate base time is the time that Symantec Protection Engine was installed. You can change the LiveUpdate base time by editing the configuration file. If you change the scheduled LiveUpdate interval, the interval adjusts based on the LiveUpdate base time.
To configure LiveUpdate to occur automatically

1. Go to the Symantec Protection Engine installation directory.
2. Enable LiveUpdate schedule.
   
   **Command:**
   
   `xmlmodifier -s //liveupdate/Schedule/@enabled true liveupdate.xml`
   
   **Allowed values:**
   
   - true
     Enables LiveUpdate.
   - false
     Disables LiveUpdate.
   
   **Default value:** true

3. In the LiveUpdate interval list, select the interval.
   
   **Command:**
   
   `xmlmodifier -s //liveupdate/Schedule/Interval/@value <value> liveupdate.xml`
   
   **Allowed values:** Any numerical value in seconds.
   
   **Default value:** 7200

4. Restart the Symantec Protection Engine service.

See “Change the LiveUpdate base time” on page 373.

See “About LiveUpdate” on page 229.

Configuring Rapid Release updates to occur automatically in the Core server only mode

You can schedule Rapid Release updates to occur automatically at a specified time interval to ensure that Symantec Protection Engine always has the most current definitions. Scheduled Rapid Release updates are disabled by default. To receive automatic Rapid Release updates, you must enable and schedule Rapid Release. When Rapid Release is scheduled, Rapid Release runs at the specified time interval that you select.

To configure Rapid Release updates to occur automatically

1. Go to the Symantec Protection Engine installation directory.
2. Configure Rapid Release updates to occur automatically.
Command:
xmlmodifier -s //liveupdate/RapidRelease/Schedule/@enabled true liveupdate.xml

Allowed values:
- true
  Enables Rapid Release updates.
- false
  Disables Rapid Release updates.

Default value: false

3 In the Rapid Release interval specify the interval between which you want Symantec Protection Engine to download Rapid Release definitions.

Command:
xmlmodifier -s //liveupdate/RapidRelease/Schedule/Interval/@value <value> liveupdate.xml

Allowed values: You can select any number between 5 minutes and 120 minutes.

Default value: 30

4 Restart the Symantec Protection Engine service.

See “About Rapid Release” on page 243.

Configuring Rapid Release to download definitions from HTTP Server

Symantec Protection Engine downloads the Rapid Release definitions from Symantec FTP server by default. You can configure it to download the definitions from HTTP server also.
To configure Rapid Release to download definitions from HTTP Server

1. Go to the Symantec Protection Engine installation directory.

2. Configure the HTTP URL.
   
   **Command:**
   
   ```bash
   xmlmodifier -s //liveupdate/RapidRelease/FTPSettings/URL/@value
   <HTTP URL> liveupdate.xml
   
   For example:
   
   Following is the default URL to download the definitions from FTP server for Windows:
   
   /norton_antivirus_corp/rapidrelease/symrapidreleasedefscore15-v5i64.exe
   
   You can change the FTP URL to the following Symantec HTTP URL:
   
   For Windows:
   
   ```bash
   xmlmodifier -s //liveupdate/RapidRelease/FTPSettings/URL/@value
   http://definitions.symantec.com/defs/rapidrelease/symrapidreleasedefscore15-v5i64.exe
   liveupdate.xml
   
   For Linux:
   
   ```bash
   xmlmodifier -s //liveupdate/RapidRelease/FTPSettings/URL/@value
   http://definitions.symantec.com/defs/rapidrelease/symrapidreleasedefscore15-unix64.sh
   liveupdate.xml
   
3. Restart the Symantec Protection Engine service.

---

**About editing the LiveUpdate XML file**

You must configure LiveUpdate in the `liveupdate.xml` file so that Symantec Protection Engine always has the most current definition files.

See “About editing the Symantec Protection Engine configuration files” on page 365.

Table 12-9 lists the default parameters that are added to the `liveupdate.xml` file.
### Table 12-9  Default Parameters in liveupdate.xml file

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| Protocol   | Updated definition files are retrieved through HTTP. This information is required unless you use a host file. The default setting for the LiveUpdate transport protocol is HTTP.  
**XPath:** /liveupdate/UpdateServer/Protocol/@value  
See “Configure the LiveUpdate server details” on page 373. |
| Server name| Symantec Protection Engine contacts a specified server to check for and to retrieve updated definition files. You must supply the appropriate LiveUpdate server name. The default server is liveupdate.symantec.com.  
**XPath:** /liveupdate/UpdateServer/Server/@value  
See “Configure the LiveUpdate server details” on page 373. |
| Server port| You must specify the TCP/IP port the LiveUpdate server server is listening on. The default value is 80.  
**XPath:** /liveupdate/UpdateServer/Port/@value  
See “Configure the LiveUpdate server details” on page 373. |
| Server path| Specify the directory on the LiveUpdate server that contains the LiveUpdate packages.  
**XPath:** /liveupdate/UpdateServer/Path/@value  
**Note:** This is an optional parameter.  
See “Configure the LiveUpdate server details” on page 373. |
Table 12-9  Default Parameters in liveupdate.xml file (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| **User name** | Specify a user name to log on to the LiveUpdate server.  
**XPath:**  
/liveupdate/UpdateServer/UserName/@value  
**Note:** This is an optional parameter.  
See “Configure the LiveUpdate server details” on page 373. |
| **Password** | Specify a password to log on to the LiveUpdate server.  
**XPath:**  
/liveupdate/UpdateServer/Password/@value  
**Note:** This is an optional parameter.  
See “Configure the LiveUpdate server details” on page 373. |
Performing a silent installation

This appendix includes the following topics:

- About silent installation and upgrade
- Implementing a silent installation in Linux
- About implementing a silent installation for Windows
- Generating an encrypted password

About silent installation and upgrade

You can use the silent installation feature to automate the installation or upgrade of Symantec Protection Engine. You can use the silent installation feature when you install or upgrade multiple Symantec Protection Engines that have identical input values.

In Linux, you can capture the required input values for installation in a response file. You can use the response file for subsequent installations to read in the values so that the installations are silent. This response file frees you from having to repeatedly supply input values for each installation.

In Windows you provide all of the information on the command-line first, and then run the installation silently.

See “Implementing a silent installation in Linux” on page 326.

See “About implementing a silent installation for Windows” on page 331.

See “Generating an encrypted password” on page 336.
Implementing a silent installation in Linux

Implementing a silent installation in Linux involves the following process:

- Create a response file to capture your input values for installation.
  See “Creating the response file” on page 326.
- Run the installation program to read the response file.
  This response file lets you perform the installation silently using the values that you specified.
  See “About initiating a silent installation using the response file” on page 331.

See “About silent installation and upgrade” on page 325.

Creating the response file

To implement a silent installation in Linux, you must create a response file that contains the parameters and input values for the required responses during installation. You can create different response files for different installation scenarios. You must create the response file before you install Symantec Protection Engine.

A default response file, called response, is included in the Symantec Protection Engine.zip file. The response file is a text file that is preconfigured with the default settings for the Symantec Protection Engine installation options. You must edit this response file so that it contains the input values that you want for the silent installation.

For silent installation to initiate, the response/no-ask-questions file must be present in the home directory of the user.

Note: Do not delete any of the parameters in the response file. The installer must read an input value for each parameter. You must specify an input value for each parameter.

Table A-1 lists the input values that are contained in the response file.
<table>
<thead>
<tr>
<th>Input name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Upgrade</td>
<td>Specifies that the installation is an upgrade.</td>
</tr>
<tr>
<td></td>
<td>- NONE</td>
</tr>
<tr>
<td></td>
<td>Use this value if you do not want to perform an upgrade. This value is the default value.</td>
</tr>
<tr>
<td></td>
<td>- UPGRADE</td>
</tr>
<tr>
<td></td>
<td>Use this value if you want to upgrade and you want to preserve your existing settings. You must configure all of the Java inputs values. All other input values are ignored.</td>
</tr>
<tr>
<td></td>
<td>- CLEAN</td>
</tr>
<tr>
<td></td>
<td>Use this value to uninstall and reinstall the product. Configure the input values that you want to modify.</td>
</tr>
<tr>
<td>AdminPort</td>
<td>The port number on which the Web-based console listens. The default port number is 8004.</td>
</tr>
<tr>
<td>AdminPassword</td>
<td>The encrypted password for the virtual administrative account that you use to manage Symantec Protection Engine.</td>
</tr>
<tr>
<td></td>
<td>The default password is <strong>changeme</strong>.</td>
</tr>
<tr>
<td></td>
<td>See “Generating an encrypted password” on page 336.</td>
</tr>
<tr>
<td>SSLPort</td>
<td>The Secure Socket Layer (SSL) port number on which encrypted files are transmitted for increased security. The default port number is 8005.</td>
</tr>
<tr>
<td>InstallDir</td>
<td>The location where to install Symantec Protection Engine. The default location is /opt/SYMCScan.</td>
</tr>
<tr>
<td>User</td>
<td>The name of an existing user under which Symantec Protection Engine runs. The default setting is root.</td>
</tr>
<tr>
<td>JavaCmd</td>
<td>The full path (can be a symlink) to the Java 2SE Runtime Environment (JRE) 8.0 (update 121 or later) 64-bit executables.</td>
</tr>
</tbody>
</table>
Table A-1  Input values in the response file (continued)

<table>
<thead>
<tr>
<th>Input name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>JavaBinDir</td>
<td>The full path (can be a symlink) to the Java 2SE Runtime Environment (JRE) 8.0 (update 121 or later) 64-bit executables. If the path is incorrect or the JRE version is not the correct version, Symantec Protection Engine does not function properly. (Symantec Protection Engine might not function properly even if the installer reports that the installation was successful.)</td>
</tr>
</tbody>
</table>
| JRELibDir        | The full path to the jre/lib/client directory. You must provide this information so that the LD_LIBRARY_PATH variable can locate the file libjvm.so. That file should exist in the following directory: ...
|                  | The JDK path is `<JDK DIR>/jre/lib/<architecture>/client/libjvm.so.` |
|                  | The JRE start path is `<JRE Dir>/lib/<architecture>/client/libjvm.so.` |
|                  | In Linux, a second library is required in the directory jre/lib/amd64. Use the shorter path. If you have installed the JDK, use `<JDK Dir>/jre/lib/amd64`. If you have installed the JRE, use `<JRE Dir>/lib/amd64`.
<p>|                  | The installer assumes that the path that you enter is correct. If the path that you provide is incorrect, Symantec Protection Engine does not function properly even if the installer reports that the installation was successful. |
| CanRelocate (Linux only) | The Boolean value that indicates the version of the Red Hat Package Manager (RPM) that you are running. If you are running RPM versions 4.0.2 or 4.1, change this setting to 0. If you are not running RPM version 4.0.2 or 4.1, do not change the default setting. The default setting is 1. |</p>
<table>
<thead>
<tr>
<th>Input name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EnableFilteringAndDownloadDefinitions</td>
<td>Enables URL Filtering and downloading of the URL definitions. Possible values are as follows:</td>
</tr>
<tr>
<td></td>
<td>■ true: Use this value if you want to enable URL filtering in filtering mode and Download URL definitions.</td>
</tr>
<tr>
<td></td>
<td>■ false: Use this value if you want to disable URL Filtering and Definition Download. This value is the default value.</td>
</tr>
<tr>
<td>UpdateServer</td>
<td>Enter the LiveUpdate server name or IP address to which you want to connect. This parameter is valid only for an upgrade where you preserve your existing settings. The default value is liveupdate.symantec.com.</td>
</tr>
<tr>
<td>UpdateServerPort</td>
<td>Enter the LiveUpdate server port number. This parameter is valid only for an upgrade where you preserve your existing settings. The default value is 80.</td>
</tr>
<tr>
<td>UpdateServerPath</td>
<td>Enter the directory path on the LiveUpdate server that contains the LiveUpdate packages. This parameter is valid only for an upgrade where you preserve your existing settings. If you do not specify a value, the default is blank.</td>
</tr>
<tr>
<td>UpdateServerProxyName</td>
<td>Enter the LiveUpdate proxy server name or IP address. This parameter is valid only for an upgrade where you preserve your existing settings. If you do not specify a value, the default is blank.</td>
</tr>
<tr>
<td>UpdateServerProxyPort</td>
<td>Enter the LiveUpdate proxy server port number. This parameter is valid only for an upgrade where you preserve your existing settings. The default value is 0.</td>
</tr>
</tbody>
</table>
Table A-1  
Input values in the response file (continued)

<table>
<thead>
<tr>
<th>Input name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>InsightAggressionLevel</strong></td>
<td>Enter the Insight aggression level. Possible values are:</td>
</tr>
<tr>
<td></td>
<td>■ 1 (Low)</td>
</tr>
<tr>
<td></td>
<td>■ 2 (Medium)</td>
</tr>
<tr>
<td></td>
<td>This is the default value.</td>
</tr>
<tr>
<td></td>
<td>■ 3 (High)</td>
</tr>
<tr>
<td><strong>Note:</strong> The Insight aggression level defines how sensitive the Symantec Insight™ feature is to a file’s reputation score.</td>
<td></td>
</tr>
<tr>
<td><strong>EnableJavaUI</strong></td>
<td>Enables the Core server with user interface feature. Possible values are:</td>
</tr>
<tr>
<td></td>
<td>■ true: Use this value if you want to use the Core server with user interface mode. This method requires JRE to be installed.</td>
</tr>
<tr>
<td></td>
<td>■ false: Use this value if you want to use the Core server only mode. This method does not require JRE to be installed.</td>
</tr>
<tr>
<td><strong>EnableURLReputationAndDownloadDefinition</strong></td>
<td>Enables URL Reputation ■ true: Enables URL Reputation and downloads URL definitions. ■ false: Disables URL Reputation</td>
</tr>
</tbody>
</table>

To create the response file for Linux

1. Locate the response file, response, in the Symantec Protection Engine.zip file and copy it to the home directory of the user.

   **Note:** For the silent installation to initiate, the response file must be located in the /home directory of the user.

2. Rename the file as no-ask-questions and open the file.

3. Supply the input value for each parameter.
   
   Make changes only to the right of the equal sign (=) for each parameter.
4 At AdminPassword=, copy and paste the encrypted string that the XML modifier command-line tool generated. Ensure that you have copied the encrypted string in its entirety. See “Generating an encrypted password” on page 336.

5 Save the file. See “Implementing a silent installation in Linux” on page 326. See “About initiating a silent installation using the response file” on page 331.

About initiating a silent installation using the response file

Ensure that the appropriate response file, called no-ask-questions, is located in the home directory of the root user. The silent installation initiates automatically if the installer finds the response file in the correct location. The existence of the no-ask-questions file in the home directory tells the installer to perform the silent installation using the input values in the file.

Note: The no-ask-questions file is not deleted after the silent installation.

See “Implementing a silent installation in Linux” on page 326. See “Creating the response file” on page 326.

About implementing a silent installation for Windows

The Symantec Protection Engine silent installation feature in Windows lets you provide the installation parameters on the command line before you run the installation. If you do not specify a value on the command-line, the default value is used.

Table A-2 lists the input values that you can use on the command line for the silent installation.

<table>
<thead>
<tr>
<th>Input name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>INSTALLDIR</td>
<td>The location to install Symantec Protection Engine. The default location is &quot;c:\Program Files\Symantec\Scan Engine&quot; for Windows platform</td>
</tr>
</tbody>
</table>
### Table A-2  Input values on the command line (continued)

<table>
<thead>
<tr>
<th>Input name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AUTHENTICATIONMODE</td>
<td>The authentication mode for accessing Symantec Protection Engine console. Possible values are as follows:</td>
</tr>
<tr>
<td></td>
<td>■ AD  Use this value if you want to use Windows Active Directory-based authentication.</td>
</tr>
<tr>
<td></td>
<td>■ SSE Use this value if you want to use Symantec Protection Engine-based authentication. This value is the default value.</td>
</tr>
<tr>
<td>GROUP_NAME</td>
<td>The fully qualified security group name in the Domain\Groupname format. This parameter is required when the authentication mode is set to Windows Active Directory-based authentication.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> During installation if value is not entered for this parameter, then you must go to configuration.xml and enter a valid security group name in correct format.</td>
</tr>
<tr>
<td>ENCRYPTED_PASSWORD</td>
<td>The encrypted password for the administrative account that you use to manage Symantec Protection Engine using the Symantec Protection Engine-based authentication. This parameter is required when the authentication mode is set to Symantec Protection Engine-based authentication.</td>
</tr>
<tr>
<td></td>
<td>The default password is <strong>changeme</strong>.</td>
</tr>
<tr>
<td></td>
<td>See &quot;Generating an encrypted password&quot; on page 336.</td>
</tr>
<tr>
<td>USERUPGRADESELECTION</td>
<td>Specifies that the installation is an upgrade. Possible values are as follows:</td>
</tr>
<tr>
<td></td>
<td>■ UPGRADE Use this value to preserve your existing settings. All other input values are ignored.</td>
</tr>
<tr>
<td></td>
<td>■ CLEAN Use this value to uninstall and reinstall the product. Configure the input values that you want to modify.</td>
</tr>
</tbody>
</table>
## Table A-2  Input values on the command line (continued)

<table>
<thead>
<tr>
<th>Input name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADMIN_PORT</td>
<td>The port number on which the Web-based console listens. The default port number is 8004.</td>
</tr>
<tr>
<td>SSL_PORT</td>
<td>The Secure Socket Layer (SSL) port number on which encrypted files are transmitted for increased security. The default port number is 8005.</td>
</tr>
<tr>
<td>ENABLE_URL_FILTERING</td>
<td>Enables URL Filtering and downloading of the URL definitions. Possible values are as follows:</td>
</tr>
<tr>
<td></td>
<td>■ true: Use this value if you want to enable URL filtering in filtering mode and Download URL definitions.</td>
</tr>
<tr>
<td></td>
<td>■ false: Use this value if you want to disable URL Filtering and Definition Download. This value is the default value.</td>
</tr>
<tr>
<td>SSE_SERVICE_ACC_PWD</td>
<td>The password for the service account if the previous Symantec Protection Engine’s service account is not Local System. This parameter is valid only for an upgrade where you preserve your existing settings. When you install Symantec Protection Engine the service does not start if this parameter is incorrect. Once the installation is complete, you should type the correct service account password and start the service manually.</td>
</tr>
<tr>
<td>UPDATE_SERVER</td>
<td>Enter the LiveUpdate server name or IP address to which you want to connect. This parameter is valid only for an upgrade where you preserve your existing settings. The default value is liveupdate.symantec.com.</td>
</tr>
<tr>
<td>UPDATE_SERVER_PORT</td>
<td>Enter the LiveUpdate server port number. This parameter is valid only for an upgrade where you preserve your existing settings. The default value is 80.</td>
</tr>
<tr>
<td>Input name</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>UPDATE_SERVER_PATH</td>
<td>Enter the directory path on the LiveUpdate server that contains the LiveUpdate packages. This parameter is valid only for an upgrade where you preserve your existing settings. If you do not specify a value, the default is blank.</td>
</tr>
<tr>
<td>UPDATE_SERVER_PROXY_NAME</td>
<td>Enter the LiveUpdate proxy server name or IP address. This parameter is valid only for an upgrade where you preserve your existing settings. If you do not specify a value, the default is blank.</td>
</tr>
<tr>
<td>UPDATE_SERVER_PROXY_PORT</td>
<td>Enter the LiveUpdate proxy server port number. This parameter is valid only for an upgrade where you preserve your existing settings. The default value is 0.</td>
</tr>
</tbody>
</table>
| INSIGHTAGGRESSIONLEVEL           | Enter the Insight aggression level. Possible values are:  
  ■ 1 (Low)  
  ■ 2 (Medium)  
  This is the default value.  
  ■ 3 (High)  
  **Note:** The Insight aggression level defines how sensitive the Symantec Insight™ feature is to a file's reputation score.                                                                                                                                                                                                                       |
| ENABLEJAVAUI                     | Enables the Core server with user interface feature. Possible values are:  
  ■ true: Use this value if you want to use the Core server with user interface mode. This method requires JRE to be installed.  
  ■ false: Use this value if you want to use the Core server only mode. This method does not require JRE to be installed.                                                                                                                                                                                                                                           |
Table A-2  Input values on the command line (continued)

<table>
<thead>
<tr>
<th>Input name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ENABLE_URL_REPUTATION</td>
<td>Enables URL Reputation</td>
</tr>
<tr>
<td></td>
<td>Possible values are:</td>
</tr>
<tr>
<td></td>
<td>■ true:</td>
</tr>
<tr>
<td></td>
<td>Enables URL Reputation and downloads URL</td>
</tr>
<tr>
<td></td>
<td>definitions.</td>
</tr>
<tr>
<td></td>
<td>■ false:</td>
</tr>
<tr>
<td></td>
<td>Disables URL Reputation</td>
</tr>
</tbody>
</table>

See “About silent installation and upgrade” on page 325.

See "Initiating a silent installation on Windows” on page 335.

Initiating a silent installation on Windows

Use the following procedures to initiate a silent installation on Windows for Symantec Protection Engine.

To initiate a silent installation on Windows

1. Change directories to the location of the Symantec Protection Engine installation program, ScanEngine.exe.

2. At the command prompt, type the following:

   ScanEngine
   /s /v"/qn <arguments>"

   where <arguments> are the input values that you want to specify.

   You must use the format <inputname>=<value> and use a space to separate each value. For example:

   ScanEngine
   /s /v"/qn USERUPGRADESELECTION=CLEAN SSL_PORT=8005"

   You must include the quotation marks in the command, or the silent installation does not function properly.

   The silent installation proceeds automatically from this point using the input values that you provide.

See “About implementing a silent installation for Windows” on page 331.
Generating an encrypted password

Use the XML modifier command-line tool to protect the administrative password that is used to manage Symantec Protection Engine. This tool encrypts the password and returns an encrypted string. You must copy the encrypted string in its entirety and paste it in the appropriate location in the response file. The XML modifier command-line tool is included on the product .zip file.

To generate an encrypted password

1. At the command prompt, type the following command:

   java -jar xmlmodifier.jar -e password

   where <password> is the password that you will use to access the Symantec Protection Engine console.

   The tool returns an encrypted string.

2. Save the entire encrypted string that the tool returns.

See “About implementing a silent installation for Windows” on page 331.
Using the Symantec Protection Engine command-line scanner

This appendix includes the following topics:

- About the Symantec Protection Engine command-line scanner
- Setting up a computer to submit files to Symantec Protection Engine for scanning
- C-based command-line scanner syntax and usage
- Java based command-line scanner syntax and usage

About the Symantec Protection Engine command-line scanner

The Symantec Protection Engine command-line scanner is a multiplatform utility that works with version 4.0.4 or later of Symantec Protection Engine. Symantec Protection Engine must be running on supported versions of Windows and Linux. The command-line scanner acts as a client to Symantec Protection Engine through the Symantec Protection Engine application programming interface (API). It uses version 1.0 of the Internet Content Adaptation Protocol (ICAP), presented in RFC 3507 (April 2003).

Symantec Protection Engine is shipped with the following command-line scanners:

- C-based command-line scanner (`ssecls.exe`) compiled using the C software development kit
  
  See “C-based command-line scanner syntax and usage” on page 339.
Java based command-line scanner (ssecls.jar) compiled using the Java software development kit
See “Java based command-line scanner syntax and usage” on page 355.

Note: The command-line scanner (ssecls.exe/ssecls.jar/ssecls binary) that is shipped with Symantec Protection Engine is meant for demonstration purposes to showcase the capabilities of the product in a limited manner. Symantec recommends that you develop your own connector application based on the SDK that is shipped with Symantec Protection Engine.

Use the command-line scanner to send files to Symantec Protection Engine to be scanned for viruses.

You can also use the command-line scanner to perform the following actions:

- Repair infected files and delete those files that are unrepairable.
- Recursively descend into subdirectories to scan multiple files.
- Obtain information about the command-line scanner and Symantec Protection Engine operation.

See “Setting up a computer to submit files to Symantec Protection Engine for scanning” on page 338.

Setting up a computer to submit files to Symantec Protection Engine for scanning

You can send files to Symantec Protection Engine by using the command-line scanner. You can run this tool from the computer on which Symantec Protection Engine is running or from a different computer. You can send files from a computer with a different operating system than the computer on which Symantec Protection Engine is installed.

To use the command-line scanner, you must select ICAP as the communication protocol for Symantec Protection Engine.

Because files are sent to Symantec Protection Engine for scanning, you can only specify files or directories for which you have the appropriate permissions. To send files, you must have read access to the files. To repair (replace) or delete files, you must have permission to modify or delete files. You must also have access to the directory where the files are located.

If you send files from the same computer on which Symantec Protection Engine runs, you do not need to install any additional files for the command-line scanner.
The appropriate files are installed automatically during the installation of Symantec Protection Engine.

You can use the command-line scanner to submit files for scanning from a computer that does not have Symantec Protection Engine installed. You must copy the command-line scanner files to the computer.

The ssecls files are organized into subdirectories by operating system. Use the files for the operating system of the computer from which you want to submit files for scanning.

Follow these procedures to set up a computer to submit files for scanning from a computer that does not have Symantec Protection Engine installed.

To set up a computer to submit files for scanning

1. Obtain copies of the command-line scanner files from one of the following locations:
   - In the Symantec Protection Engine.zip file, in the top-level Command_Line_Scanner directory.
   - On the computer on which Symantec Protection Engine is installed, in the Symantec Protection Engine installation directory, in the ssecls subdirectory (Linux) or CmdLineScanner subdirectory (Windows).

2. Copy the entire contents of the directory for the appropriate operating system.

3. On the computer from which you want to submit files for scanning, place the files in a directory location that is in the command prompt path.

See “About the Symantec Protection Engine command-line scanner” on page 337.
See “C-based command-line scanner syntax and usage” on page 339.

C-based command-line scanner syntax and usage

The C-based command-line scanner of Symantec Protection Engine uses the following general syntax:

```
sscl [-options] <path> [...]
```

The <path> parameter lets you specify one or more files or directories to scan. Each file or directory must be separated by spaces. You can use the absolute or relative path. If the specified path is to a file, the file is scanned. If the path is to a directory, all of the files in the directory are scanned.

**Note:** Do not use a path with a symbolic link. Symantec Protection Engine does not follow a symbolic link to a file.
You can specify any combination of files and directories. You must separate multiple entries with a space. For example:

```
sscls [-options] <pathtofile1> <pathtofile2> <pathtofile3>
```

You can specify any mounted file system, mount point, or mapped drive. For example:

```
C:\Work\Scantest.exe
/export/home/
```

Follow the standard formats for your operating system for handling path names (for example, special characters, quotation marks, or wildcard characters).

If you have specified a directory for scanning and want Symantec Protection Engine to descend into subdirectories to scan additional files, you must also use the -recurse option.


You can only specify files or directories for which you have appropriate permissions. To send files, you must have read access to the files. To repair (replace) or delete files, you must have permission to modify or delete the files. You must also have access to the directory where the files are located.

If you do not specify a path, input data is read from standard input (STDIN) and sent to Symantec Protection Engine for scanning. After the scan, the data (either the original file, if it was clean, or the repaired file) is written to standard output (STDOUT). If a file is infected and cannot be repaired, no data is written to STDOUT.

---

**Note:** DBCS path names in scan requests should not be converted to Unicode (UTF-8) encoding before the path is passed to Symantec Protection Engine.

---

See "About the Symantec Protection Engine command-line scanner" on page 337.

See "Setting up a computer to submit files to Symantec Protection Engine for scanning" on page 338.

See "Supported command-line options for C-based command-line scanner" on page 341.

See "About specifying the Symantec Protection Engine IP address and port for C-based command-line scanner" on page 346.

See "About specifying the antivirus scanning mode for C-based command-line scanner" on page 347.

See "About obtaining scan results for C-based command-line scanner" on page 347.

See “About disposing of infected files when an error occurs” on page 351.
See “Excluding files from scanning” on page 351.
See “Redirecting console output to a log file” on page 352.
See “About scanning files in Symantec Protection Engine using different services/APIs” on page 353.
See “About using Insight command options with C-based command-line scanner” on page 354.

Supported command-line options for C-based command-line scanner

Table B-1 describes the options that the command-line scanner supports.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| -server | Specify one or more Symantec Protection Engines for scanning files. You must separate multiple entries with a semicolon. If you do not specify a Symantec Protection Engine, the server option defaults to the local host that listens on the default port.

The format for each Symantec Protection Engine is <IPaddress:port>, where IPaddress is the DNS name or IP address of the computer on which Symantec Protection Engine is running, and port is the port number on which Symantec Protection Engine listens.

**Note:** When more than one Symantec Protection Engine is specified, the load balancing and failover features of the API are activated automatically.

See “About specifying the Symantec Protection Engine IP address and port for C-based command-line scanner” on page 346.
### Table B-1  Supported options for the C-based command-line scanner (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-mode</td>
<td>Optionally override the default antivirus scanning mode.</td>
</tr>
<tr>
<td></td>
<td>The scanning modes that you can select are as follows:</td>
</tr>
<tr>
<td></td>
<td>■ Scanrepairdelete</td>
</tr>
<tr>
<td></td>
<td>If you do not specify a scanning mode, the scan policy defaults to scanrepairdelete. Symantec Protection Engine tries to repair infected files. Files that cannot be repaired are deleted. This configuration is the recommended setting.</td>
</tr>
<tr>
<td></td>
<td>■ Scan</td>
</tr>
<tr>
<td></td>
<td>Files are scanned, but no repair is tried. Infected files are not deleted.</td>
</tr>
<tr>
<td></td>
<td>■ Scanrepair</td>
</tr>
<tr>
<td></td>
<td>Symantec Protection Engine tries to repair infected files. Files that cannot be repaired are not deleted.</td>
</tr>
<tr>
<td></td>
<td>See &quot;About specifying the antivirus scanning mode for C-based command-line scanner&quot; on page 347.</td>
</tr>
<tr>
<td>-verbose</td>
<td>Report detailed information about the file that is scanned.</td>
</tr>
<tr>
<td></td>
<td>When you use this option, a line of output is printed to STDOUT for each file that is scanned. The information includes both the name of the file and the result of the scan, including the final disposition of the file.</td>
</tr>
<tr>
<td></td>
<td>See &quot;About using the -verbose option&quot; on page 348.</td>
</tr>
<tr>
<td>-details</td>
<td>Report detailed information about the infections or violations that are found.</td>
</tr>
<tr>
<td></td>
<td>When you use this option, a block of text is printed to STDOUT for each file that is scanned. The output text indicates the name of the file that was scanned and the result of the scan. If the file is infected or violates an established policy, the output text also provides information about the violation or infection.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If you use the -details option, you do not need to use the -verbose option. The output for the -verbose option is duplicated as part of the output for the -details option.</td>
</tr>
<tr>
<td></td>
<td>See &quot;About using the -details option&quot; on page 349.</td>
</tr>
</tbody>
</table>
Table B-1  Supported options for the C-based command-line scanner (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-timing</code></td>
<td>Report the time that was required to scan a file. When you use this option, a line of output is printed to STDOUT for each file that is scanned. The output includes the name of the file that was scanned and the time that it took Symantec Protection Engine to scan the file. See &quot;About using the <code>-timing</code> option&quot; on page 350.</td>
</tr>
<tr>
<td><code>-recurse</code></td>
<td>Recursively descend into the subdirectories that are inside each path that is specified on the command line. See &quot;About requesting recursive scanning&quot; on page 350.</td>
</tr>
<tr>
<td><code>-onerror</code></td>
<td>Specify the disposition of a file that has been modified (repaired) by Symantec Protection Engine when an error occurs when Symantec Protection Engine replaces a file. The default setting is to delete the file. You can specify one of the following:  - Leave  The original (infected) file is left in place.  - Delete  The original (infected) file is deleted, even though the replacement data is unavailable. See &quot;About disposing of infected files when an error occurs&quot; on page 351.</td>
</tr>
<tr>
<td><code>-exclude</code></td>
<td>Specify a path of rule file to exclude certain files from scanning. You can exclude files by name from being scanned. See &quot;Excluding files from scanning&quot; on page 351.</td>
</tr>
<tr>
<td><code>-maxsize</code></td>
<td>Specify maximum file size in bytes to exclude the files that exceed a limit from being scanned. Files that exceed the maximum file size limit are not sent to Symantec Protection Engine for scanning. See &quot;Excluding files from scanning&quot; on page 351.</td>
</tr>
</tbody>
</table>
Table B-1  Supported options for the C-based command-line scanner (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-log</td>
<td>The command-line scanner redirects the console output to a log file. When the scan finishes, Symantec Protection Engine writes a summary to the log file (if you are running in log mode) and the screen. The summary shows the number of files that were scanned and the number of viruses found. See “Redirecting console output to a log file” on page 352.</td>
</tr>
</tbody>
</table>
| -api     | The command-line scanner now includes services for supporting Symantec Insight™, better categorization of threats, and unscannable file handling features. You can specify one of the following options:  
  - 0: Scan file with legacy API's.  
  - Note: This is the default value.  
  - 1: Scan file with enhanced threat categorization API's.  
  - 2: Scan file with Insight API's. See “About scanning files in Symantec Protection Engine using different services/APIs” on page 353. |
| -disableinsight | Disable the Symantec Insight feature.  
  - Note: This service is applicable only if -api = 2. See “About using Insight command options with C-based command-line scanner” on page 354. |
| -digitallysigned | Specify if the file is digitally signed.  
  - Note: This service is applicable only if -api = 2. You can specify one of the following options:  
  - 0: File is not digitally signed.  
  - 1: File is digitally signed. See “About using Insight command options with C-based command-line scanner” on page 354. |
| -SHA256  | Specify the SHA256 value of the file.  
  - Note: This service is applicable only if -api = 2. See “About using Insight command options with C-based command-line scanner” on page 354. |
Table B-1  Supported options for the C-based command-line scanner
*(continued)*

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-MD5Hash</td>
<td>Specify the MD5 value of the file.</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>This service is applicable only if <code>-api = 2</code>.</td>
</tr>
<tr>
<td></td>
<td>See “About using Insight command options with C-based command-line scanner” on page 354.</td>
</tr>
<tr>
<td>-SourceIP</td>
<td>Specify the source IP of the file.</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>This service is applicable only if <code>-api = 2</code>.</td>
</tr>
<tr>
<td></td>
<td>See “About using Insight command options with C-based command-line scanner” on page 354.</td>
</tr>
<tr>
<td>-SourceURL</td>
<td>Specify the source URL of the file.</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>This service is applicable only if <code>-api = 2</code>.</td>
</tr>
<tr>
<td></td>
<td>See “About using Insight command options with C-based command-line scanner” on page 354.</td>
</tr>
<tr>
<td>-aggressionlevel</td>
<td>Specify the Insight aggression level.</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>This service is applicable only if <code>-api = 2</code>.</td>
</tr>
<tr>
<td></td>
<td>You can specify one of the following options:</td>
</tr>
<tr>
<td>■ 1: Low</td>
<td><strong>Note:</strong> This is the default value.</td>
</tr>
<tr>
<td>■ 2: Medium</td>
<td>■ 3: High</td>
</tr>
<tr>
<td></td>
<td>See “About using Insight command options with C-based command-line scanner” on page 354.</td>
</tr>
<tr>
<td>-reportinsightinfo</td>
<td>Enable or disable the Insight information for the file.</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>This service is applicable only if <code>-api = 2</code>.</td>
</tr>
<tr>
<td></td>
<td>You can specify one of the following options:</td>
</tr>
<tr>
<td>■ 0: Symantec Protection Engine does not provide reputation information in ICAP response.</td>
<td></td>
</tr>
<tr>
<td>■ 1: Symantec Protection Engine provides information in ICAP response for Insight convicted files.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>See “About using Insight command options with C-based command-line scanner” on page 354.</td>
</tr>
</tbody>
</table>
About specifying the Symantec Protection Engine IP address and port for C-based command-line scanner

The -server option lets you specify one or more Symantec Protection Engines for scanning files. If you do not specify a Symantec Protection Engine, the server defaults to the local host that listens on the default port.

The format for each Symantec Protection Engine entry is <IPaddress:port>, where IPaddress is the DNS name or IP address of the computer on which Symantec Protection Engine is running, and port is the port number on which Symantec Protection Engine listens. You only need to specify the port number if Symantec Protection Engine is installed on a port other than the default. (The default port number for ICAP is 1344.) For example:

`ssecls -server 192.168.0.100 c:\temp`

`ssecls -server 192.168.0.100:5555 c:\temp`

You can specify multiple Symantec Protection Engines. You must separate multiple entries with a semicolon. For example:

`ssecls -server 192.168.0.100:1344;192.168.0.101:1344 c:\temp`

When more than one Symantec Protection Engine is specified, the load balancing and failover features of the API are activated automatically. The Symantec Protection Engine API provides scheduling across any number of computers that are running Symantec Protection Engine. When multiple Symantec Protection Engines are used, the API determines which Symantec Protection Engine should receive the next file based on the scheduling algorithm.

If a Symantec Protection Engine is unreachable or stops responding during a scan, another Symantec Protection Engine is called. The faulty Symantec Protection Engine is taken out of rotation for 30 seconds. If all of Symantec Protection Engines are out of rotation, the faulty Symantec Protection Engines are called again.

The API does not stop trying to contact Symantec Protection Engine unless any of the following conditions occur:

- At least five engines do not function.
- It appears that a file that was scanned might have caused more than one engine to stop responding.

See “C-based command-line scanner syntax and usage” on page 339.

See “Supported command-line options for C-based command-line scanner” on page 341.
About specifying the antivirus scanning mode for C-based command-line scanner

The -mode option lets you override the default antivirus scanning mode for the command-line scanner. The default scanning mode is `scanrepairdelete`. Symantec Protection Engine tries to repair infected files. Files that cannot be repaired are deleted.

You do not need to specify an antivirus scanning mode to use the default setting. `Scanrepairdelete` is the recommended setting.

To override the default antivirus scanning mode, you can specify one of the following scanning modes using the -mode option:

- **Scan**
  - Files are scanned, but no repair is tried. Infected files are not deleted.

- **Scanrepair**
  - Symantec Protection Engine tries to repair infected files. Files that cannot be repaired are not deleted.

For example:

```
sscls -server 192.168.0.100:1344 -mode scanrepair c:\temp
```

When files are sent to Symantec Protection Engine using the command-line scanner, the command-line scanning mode overrides the scan policy configuration on Symantec Protection Engine. This override includes scanning the files that are embedded in container files. If you do not specify a scanning mode using the -mode option, the default setting (`scanrepairdelete`) applies.

See "C-based command-line scanner syntax and usage" on page 339.

See "Supported command-line options for C-based command-line scanner" on page 341.

About obtaining scan results for C-based command-line scanner

Use the following options to obtain detailed information about a scan:

- **-verbose**
  - See “About using the -verbose option” on page 348.

- **-details**
  - See “About using the -details option” on page 349.

- **-timing**
  - See “About using the -timing option” on page 350.

These options are not available if you use the pipe mode to send a file for scanning.
About using the -verbose option

Use the -verbose option to obtain information about each file that is scanned. When this option is used, a line of output is printed to STDOUT for each file. The information includes the name of the file, the result of the scan, and the final disposition of the file. For example, consider the following command:

```bash
ssecls -server 192.168.0.100:1344 -verbose c:\work\filea c:\work\fileb
c:\work\filec c:\work\filed
```

Table B-2 lists the possible scan result codes.

<table>
<thead>
<tr>
<th>Result code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-2</td>
<td>An error occurred within Symantec Protection Engine. The file was not scanned.</td>
</tr>
<tr>
<td>-1</td>
<td>An error occurred within the command-line scanner. The file was not scanned.</td>
</tr>
</tbody>
</table>
| 0           | The file was successfully scanned and is clean. This code can have any of the following meanings:  
|             | - The file was not infected.  
|             | - The file was infected and repaired.  
|             | - The file was a container file that contains the embedded files that were infected and were repaired or deleted. |
| 1           | The file was successfully scanned, was not able to be repaired, and was not deleted. This result code can mean either that the file was unrepairable or that the scan policy did not allow repair. |
| 2           | The file was successfully scanned, was not able to be repaired, and was deleted. This result code can mean either that the file was unrepairable or that the scan policy did not permit repair. |

The output when four files (for example, a, b, c, and d) are scanned should look similar to the following:

```bash
c:\work\filea -1
c:\work\fileb 2
c:\work\filec 2
c:\work\filed 0
```

See “C-based command-line scanner syntax and usage” on page 339.
See “Supported command-line options for C-based command-line scanner” on page 341.

**About using the -details option**

Use the -details option to obtain information about the infections or violations that are found. When this option is used, a block of text is printed to STDOUT for each file that is infected or that violates an established policy. The output text indicates the name of the file, information about the infection or the violation, and the result of the scan. For example, consider the following command:

```
ssecls -server 192.168.0.100:1344 -details c:\work\filea c:\work\fileb c:\work\filec c:\work\filed
```

The output includes the following information:

<table>
<thead>
<tr>
<th>Problem name</th>
<th>Virus name or description of the container violation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Problem ID</td>
<td>Virus ID for viruses or pseudo-ID for policy violations</td>
</tr>
<tr>
<td>Disposition</td>
<td>Infected, repaired, or deleted</td>
</tr>
</tbody>
</table>

**Note:** The output data mirrors the information that Symantec Protection Engine returns for each infection or violation that is identified. It might not reflect the final disposition of the file. The code for the scan results indicates the final disposition of the file. This information is also displayed when you use the -verbose option.

The output when four files (for example, a, b, c, and d) are scanned and files c and d are found to be infected with the Kakworm.c virus should look similar to the following example:

```
c:\work\filec 2
Kakworm.c
2832
Infected
```
```
c:\work\filed 2
Kakworm.c
2832
Infected
```

See “C-based command-line scanner syntax and usage” on page 339.
About using the -timing option

Use the -timing option to examine the time that is required to scan each file. For example, consider the following command:

```
ssecls -server 192.168.0.100:1344 -timing c:\work\filea c:\work\fileb c:\work\filec c:\work\filed
```

When this option is used, a line of output is printed to STDOUT for each file that is scanned. The output includes the name of the file that was scanned and the time that it took Symantec Protection Engine to scan the file.

The reported scan time is calculated as the elapsed time between when the connection with Symantec Protection Engine opens and closes. The time is reported in seconds with millisecond accuracy.

The output when four files (for example, a, b, c, and d) are scanned should look similar to the following example:

```
c:\work\filea 0.018s

c:\work\fileb 0.013s

c:\work\filec 0.43s

c:\work\filed 0.03s
```

See “Supported command-line options for C-based command-line scanner” on page 341.

About requesting recursive scanning

Use the -recurse option to recursively descend into the subdirectories that are inside each path that is specified on the command line. By default, the command-line scanner does not recursively search directories for files to send to Symantec Protection Engine for scanning. You must use the -recurse option to do so, as in the following example:

```
ssecls -server 192.168.0.100:1344 -recurse c:\winnt
```

Note: The recursive option does not apply when you use pipe mode.

See “C-based command-line scanner syntax and usage” on page 339.
About disposing of infected files when an error occurs

The -onerror option specifies how to dispose of a file that Symantec Protection Engine has repaired but that then experienced an error when trying to replace the file. The default setting is to delete the file.

You can specify one of the following settings:

- **Leave**: The original (infected) file is left in place.
- **Delete**: The original (infected) file is deleted, even though the replacement data is unavailable.

For example:

```
ssecls -server 192.168.0.100:1344 -onerror delete c:\temp
```

**Note**: This option does not apply when you use pipe mode.

Excluding files from scanning

Use the command-line scanner to exclude certain files from scanning. When the scan finishes, Symantec Protection Engine writes a summary to the log file (if you are running in log mode) and to the screen. The summary shows the number of files that were scanned and the number of viruses found.

You can use the command-line scanner to exclude files in the following ways:

- Exclude the files that exceed a limit from being scanned
- Exclude files by name from being scanned
To exclude the files that exceed a limit from being scanned

◆ Type the following argument:

   -maxsize _bytes_

   where <bytes> is the maximum file size to be scanned.

   Files that exceed the maximum file size limit are not sent to Symantec Protection Engine for scanning.

To exclude files by name from being scanned

◆ Type the following argument:

   -exclude _path_

   where <path> is the path to the rule file.

   The format for a rule file is one string per line, where the string can contain one of the following:

   | File name | All files by that file name are excluded from scanning regardless of the folders in which they are found. To exclude all files with a specific extension, use *.ext. (This instance is the only supported use of a wildcard character.) For example, memo.doc. |
   | Full path name | Only this specific file is excluded from scanning. For example, C:/Programs/memo.doc |
   | Full directory path names | Every file in this directory is excluded from scanning. For example, C:/Programs |

See “C-based command-line scanner syntax and usage” on page 339.

Redirecting console output to a log file

Use the command-line scanner to redirect console output to a log file. When the scan finishes, Symantec Protection Engine writes a summary to the log file (if you are running in log mode) and the screen. The summary shows the number of files that were scanned and the number of viruses found.
To redirect console output to a log file

- Type the following argument:
  
  `-log <_path_>`

  where `<path>` is a full or partial path to a file.

  The file is created if it does not exist. If the file exists, it is overwritten. Most output is sent to the log file instead of the screen when you use in this mode. Ssecls writes a series of dots to the screen as it scans files so that you can view the progress.

  See “C-based command-line scanner syntax and usage” on page 339.

About scanning files in Symantec Protection Engine using different services/APIs

Symantec Protection Engine now includes services for supporting Insight, better categorization of threats and unscannable file handling features. These services provide Insight information, additional threat information and unscannable file count in ICAP response. For more information, see the Symantec Protection Engine Software Developer’s Guide.

The `-api` option specifies what service to use to scan the file. The default setting is to use the old API to scan files.

Table B-3 describes options for scanning files in Symantec Protection Engine.

### Table B-3  Options to scan file in Symantec Protection Engine

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| 0      | Scan file with legacy API's.  
  **Note:** This is the default value. |
| 1      | Scan file with enhanced threat categorization API's. |
| 2      | Scan file with Insight API's. |

For example:

```plaintext
ssecls -server 192.168.0.100:1344 -api 1 c:\test.txt
ssecls -server 192.168.0.100:1344 -api 1 /test.txt
```

See “C-based command-line scanner syntax and usage” on page 339.

See “Supported command-line options for C-based command-line scanner” on page 341.
About using Insight command options with C-based command-line scanner

*Table B-4* explains the insight-specific command options that can be set from the command-line scanner at run time.

**Note:** The command options explained in *Table B-4* are optional. To use these Insight command options, make sure that you set the value of `-api` to 2.

<table>
<thead>
<tr>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-disableinsight</code></td>
<td>This command option lets you specify if you want to enable/disable Insight. If Insight is disabled, all other Insight-specific command options are ignored.</td>
</tr>
<tr>
<td><code>-digitallysigned</code></td>
<td>This command option lets you specify if the file is digitally signed or not. By default, Symantec Protection Engine checks if the file is digitally signed or not. If the file is not digitally signed, it saves on the time that Symantec Protection Engine takes to check the digital signature information. This improves the Insight query performance.</td>
</tr>
<tr>
<td><code>-SHA256</code></td>
<td>This command option lets you specify the SHA256 hash value of the file. Symantec Protection Engine calculates the SHA256 value, if not provided. You may want to provide the SHA256 value to save on the time taken to calculate the SHA256 value.</td>
</tr>
<tr>
<td><code>-MD5Hash</code></td>
<td>This command option lets you specify the MD5 hash value of the file. If specified Symantec Protection Engine may use it for the Insight query.</td>
</tr>
<tr>
<td><code>-SourceIP</code></td>
<td>This command option lets you specify the IP address of the source from where the file is downloaded.</td>
</tr>
<tr>
<td><code>-SourceURL</code></td>
<td>This command option lets you specify the URL of the source from where the file is downloaded.</td>
</tr>
<tr>
<td><code>-aggressionlevel</code></td>
<td>This command option lets you set the Insight aggression level. The Insight aggression level defines how sensitive the Symantec Insight™ feature is to a file's reputation score.</td>
</tr>
</tbody>
</table>
Table B-4  Insight command options  (continued)

<table>
<thead>
<tr>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-reportinsightinfo</td>
<td>This command option decides if Insight information should be made available in the response or not.</td>
</tr>
</tbody>
</table>

Example:

```
sscle -api 2 -digitallysigned 1 -SHA256 63ac0ad9c9dbef0da4c07c3c685dce4d41a4169eb5efaf9347dd577d3270d -MD5Hash 62825AA34568DA314E6D2AC2ACD2181 -SourceIP "192.172.1.8" -SourceURL"www.symantec.com" -reportinsightinfo 1 -aggressionlevel 2 c:\testfolder\test.exe
```

See “Supported command-line options for C-based command-line scanner” on page 341.

See “C-based command-line scanner syntax and usage” on page 339.

### Java based command-line scanner syntax and usage

The Java based command-line scanner of Symantec Protection Engine uses the following general syntax:

```
java -jar ssecls.jar [options] -f <file to scan>
```

The `<file to scan>` parameter lets you specify a file to scan. You can use the absolute or relative path.

**Note:** Do not use a path with a symbolic link. Symantec Protection Engine does not follow a symbolic link to a file.

You can specify any mounted file system, mount point, or mapped drive. For example:

```
C:\Work\Scantest.exe
/export/home/
```

Follow the standard formats for your operating system for handling path names (for example, special characters, quotation marks, or wildcard characters).

You can only specify files for which you have appropriate permissions. To send files, you must have read access to the files. To repair (replace) or delete files, you must have permission to modify or delete the files. You must also have access to the directory where the files are located.
Supported command-line options for Java based command-line scanner

Table B-5 describes the options that the command-line scanner supports.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-s, --server</td>
<td>Specify one or more Symantec Protection Engines for scanning files. You must separate multiple entries with a semicolon and the entries should be in double quotes. If you do not specify a Symantec Protection Engine, the server option defaults to the local host that listens on the default port. The format for each Symantec Protection Engine is &lt;IP address:port&gt;, where IP address is the DNS name or IP address of the computer on which Symantec Protection Engine is running, and port is the port number on which Symantec Protection Engine listens. <strong>Note:</strong> When more than one Symantec Protection Engine is specified, the load balancing and failover features of the API are activated automatically. See “About specifying the Symantec Protection Engine IP address and port for Java based command-line scanner” on page 359.</td>
</tr>
</tbody>
</table>
### Supported options for the Java based command-line scanner (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-a, --action</td>
<td>Optionally override the default antivirus scanning mode. The scanning modes that you can select are as follows:</td>
</tr>
<tr>
<td></td>
<td>- Scan Files are scanned, but no repair is tried. Infected files are not deleted.</td>
</tr>
<tr>
<td></td>
<td>- Scanrepair Symantec Protection Engine tries to repair infected files. Files that cannot be repaired are not deleted.</td>
</tr>
<tr>
<td></td>
<td>- Scanrepairdelete Symantec Protection Engine tries to repair infected files. Files that cannot be repaired are deleted. This configuration is the recommended setting.</td>
</tr>
<tr>
<td></td>
<td>- Default If you do not specify a scanning mode, the scan policy defaults to the policy set on the Symantec Protection Engine.</td>
</tr>
<tr>
<td></td>
<td>See “About specifying the antivirus scanning mode for Java based command-line scanner” on page 360.</td>
</tr>
<tr>
<td>-c, --clobber</td>
<td>Always overwrites the scanned file with server response.</td>
</tr>
<tr>
<td>-b, --verbose</td>
<td>Report detailed information about the file that is scanned. When you use this option, a line of output is printed to STDOUT for each file that is scanned. The information includes both the name of the file and the result of the scan, including the final disposition of the file.</td>
</tr>
<tr>
<td></td>
<td>See “About using the --verbose option in the java based command-line scanner” on page 361.</td>
</tr>
<tr>
<td>-p, --api</td>
<td>The command-line scanner now includes services for supporting Insight, better categorization of threats, and unscannable file handling features.</td>
</tr>
<tr>
<td></td>
<td>You can specify one of the following options:</td>
</tr>
<tr>
<td></td>
<td>- 0: Scan file with legacy API's. This is the default value.</td>
</tr>
<tr>
<td></td>
<td>- 1: Scan file with APIs (enhanced threat categorization).</td>
</tr>
<tr>
<td></td>
<td>- 2: Scan file with Insight API's.</td>
</tr>
<tr>
<td></td>
<td>See “About scanning files in Symantec Protection Engine using different services/APIs with Java based command-line scanner” on page 362.</td>
</tr>
</tbody>
</table>
### Table B-5  
Supported options for the Java based command-line scanner  
*(continued)*

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| `-d, --disableinsight` | Disable the Symantec Insight feature.  
*Note:* This service is applicable only if `-p, --api = 2`.  
See “About using Insight command options with Java based command-line scanner” on page 362. |
| `-l, --aggressionlevel` | Specify the Insight aggression level.  
*Note:* This service is applicable only if `-p, --api = 2`.  
You can specify one of the following options:  
- 1: Low  
  *Note:* This is the default value.  
- 2: Medium  
- 3: High  
See “About using Insight command options with Java based command-line scanner” on page 362. |
| `-md5, --md5hash` | Specify the MD5 value of the file.  
*Note:* This service is applicable only if `-p, --api = 2`.  
See “About using Insight command options with Java based command-line scanner” on page 362. |
| `-sha, --sha256` | Specify the SHA256 value of the file.  
*Note:* This service is applicable only if `-p, --api = 2`.  
See “About using Insight command options with Java based command-line scanner” on page 362. |
| `-i, --sourceip` | Specify the source IP of the file.  
*Note:* This service is applicable only if `-p, --api = 2`.  
See “About using Insight command options with Java based command-line scanner” on page 362. |
| `-u, --sourceurl` | Specify the source URL of the file.  
*Note:* This service is applicable only if `-p, --api = 2`.  
See “About using Insight command options with Java based command-line scanner” on page 362. |
### Table B-5

**Supported options for the Java based command-line scanner (continued)**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-n, --digitallysigned</code></td>
<td>Specify if the file is digitally signed.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This service is applicable only if <code>-p, --api = 2</code>.</td>
</tr>
<tr>
<td></td>
<td>You can specify one of the following options:</td>
</tr>
<tr>
<td></td>
<td>0: File is not digitally signed.</td>
</tr>
<tr>
<td></td>
<td>1: File is digitally signed.</td>
</tr>
<tr>
<td></td>
<td>See “About using Insight command options with Java based command-line scanner” on page 362.</td>
</tr>
<tr>
<td><code>-r, --reportinsightinfo</code></td>
<td>Specify the Insight information for the file.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This service is applicable only if <code>-p, --api = 2</code>.</td>
</tr>
<tr>
<td></td>
<td>You can specify one of the following options:</td>
</tr>
<tr>
<td></td>
<td>0: Symantec Protection Engine does not provide reputation information in ICAP response.</td>
</tr>
<tr>
<td></td>
<td>1: Symantec Protection Engine provides information in ICAP response for Insight convicted files.</td>
</tr>
<tr>
<td></td>
<td>See “About using Insight command options with Java based command-line scanner” on page 362.</td>
</tr>
</tbody>
</table>

See “Java based command-line scanner syntax and usage” on page 355.

### About specifying the Symantec Protection Engine IP address and port for Java based command-line scanner

The `-server` option lets you specify one or more Symantec Protection Engines for scanning files. If you do not specify a Symantec Protection Engine, the server defaults to the local host that listens on the default port.

The format for each Symantec Protection Engine entry is `<IPaddress:port>`, where IPaddress is the DNS name or IP address of the computer on which Symantec Protection Engine is running, and port is the port number on which Symantec Protection Engine listens. You only need to specify the port number if Symantec Protection Engine is installed on a port other than the default. (The default port number for ICAP is 1344.) For example:

- `java -jar ssecls.jar --server 192.168.0.100 -f c:\temp\abc.txt`
- `java -jar ssecls.jar --server 192.168.0.100:5555 -f c:\temp\abc.txt`
You can specify multiple Symantec Protection Engines. You must separate multiple entries with a semicolon and you must enclose the entries in double quotes. For example:

```
java -jar ssecls.jar --server "192.168.0.100:1344;192.168.0.101:1344" -f c:\temp\abc.txt
```

When more than one Symantec Protection Engine is specified, the load balancing and failover features of the API are activated automatically. The Symantec Protection Engine API provides scheduling across any number of computers that are running Symantec Protection Engine. When multiple Symantec Protection Engines are used, the API determines which Symantec Protection Engine should receive the next file based on the scheduling algorithm.

If a Symantec Protection Engine is unreachable or stops responding during a scan, another Symantec Protection Engine is called. The faulty Symantec Protection Engine is taken out of rotation for 30 seconds. If all of Symantec Protection Engines are out of rotation, the faulty Symantec Protection Engines are called again.

The API does not stop trying to contact Symantec Protection Engine unless any of the following conditions occur:

- At least five engines do not function
- It appears that a file that was scanned might have caused more than one engine to stop responding

See “Java based command-line scanner syntax and usage” on page 355.

See “Supported command-line options for Java based command-line scanner” on page 356.

About specifying the antivirus scanning mode for Java based command-line scanner

The --action option lets you override the default antivirus scanning mode for the Java based command-line scanner. The default scanning mode is the antivirus scan policy set on the Symantec Protection Engine.

You do not need to specify an antivirus scanning mode to use the default setting. "Scanrepairdelete" is the recommended setting.

To override the default antivirus scanning mode, you can specify one of the following scanning modes using the -action option:

- **Scan** Files are scanned, but no repair is tried. Infected files are not deleted.
- **Scanrepair** Symantec Protection Engine tries to repair infected files. Files that cannot be repaired are not deleted.
Scanrepair delete Symantec Protection Engine tries to repair infected files. Files that cannot be repaired are deleted.

For example:

```
java -jar ssecls.jar --server 192.168.0.100:1344 --action scanrepair -f c:\temp\abc.txt
```

When files are sent to Symantec Protection Engine using Java based command-line scanner, the command-line scanning mode overrides the scan policy configuration on Symantec Protection Engine. This override includes scanning the files that are embedded in container files. If you do not specify a scanning mode using the --action option, the default setting is the antivirus scan policy set on Symantec Protection Engine.

See “Java based command-line scanner syntax and usage” on page 355.

See “Supported command-line options for Java based command-line scanner” on page 356.

About obtaining scan results for Java based command-line scanner

You can use the --verbose option to obtain detailed information about a scan.

See “About using the --verbose option in the java based command-line scanner” on page 361.

This option is not available if you use the pipe mode to send a file for scanning.

About using the --verbose option in the java based command-line scanner

Use the --verbose option to obtain information about each file that is scanned. When this option is used, a line of output is printed to STDOUT for each file. The information includes the name of the file, the result of the scan, and the final disposition of the file. For example, consider the following command:

```
java -jar ssecls.jar --server 192.168.0.100:1344 --verbose -f c:\work\filea
```

The output when a file scanned using the --verbose option should look similar to the following:

File Scanned: c:\work\filea

Scan Status: Clean

See “Java based command-line scanner syntax and usage” on page 355.
See “About obtaining scan results for Java based command-line scanner” on page 361.

See “Supported command-line options for Java based command-line scanner” on page 356.

About scanning files in Symantec Protection Engine using different services/APIs with Java based command-line scanner

Symantec Protection Engine now includes services for supporting Insight, better categorization of threats and unscannable file handling features. These services provide Insight information, additional threat information and unscannable file count in ICAP response. For more information, see the Symantec Protection Engine Software Developer’s Guide.

The -api option specifies what service to use to scan the file. The default setting is to use the old API to scan files.

Table B-6 describes the options to scan file in Symantec Protection Engine.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| 0      | Scan file with legacy API's.  
  Note: This is the default value. |
| 1      | Scan file with enhanced threat categorization API's. |
| 2      | Scan file with Insight API's. |

For example:

```
java -jar ssecls.jar --server 192.168.0.100:1344 --api 1 -f c:\temp\test.txt
java -jar ssecls.jar --server 192.168.0.100:1344 --api 1 -f /test.txt
```

See “Java based command-line scanner syntax and usage” on page 355.

See “Supported command-line options for Java based command-line scanner” on page 356.

About using Insight command options with Java based command-line scanner

Table B-7 explains the insight-specific command options that can be set from the command-line scanner at run time.
Note: The command options explained in Table B-7 are optional. To use these Insight command options, make sure that you set the value of -api to 2.

Table B-7  Insight command options

<table>
<thead>
<tr>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
</table>
| -d, --disableinsight | This command option lets you specify if you want to enable/disable Insight.  
If Insight is disabled, all other Insight-specific command options are ignored. |
| -n, --digitallysigned | This command option lets you specify if the file is digitally signed or not. By default, Symantec Protection Engine checks if the file is digitally signed or not.  
If the file is not digitally signed, it saves on the time that Symantec Protection Engine takes to check the digital signature information. This improves the Insight query performance. |
| -sha, --sha256 | This command option lets you specify the SHA256 hash value of the file. Symantec Protection Engine calculates the SHA256 value, if not provided.  
You may want to provide the SHA256 value to save on the time taken to calculate the SHA256 value. |
| -md5, --md5Hash | This command option lets you specify the MD5 hash value of the file. Symantec Protection Engine may use it for the Insight query. |
| -i, --sourceip | This command option lets you specify the IP address of the source from where the file is downloaded. |
| -u, --sourceurl | This command option lets you specify the URL of the source from where the file is downloaded. |
| -l, --aggressionlevel | This command options lets you set the Insight aggression level. The Insight aggression level defines how sensitive the Symantec Insight™ feature is to a file's reputation score. |
| -r, --reportinsightinfo | This command option decides if Insight information should be made available in the response or not. |

Example:
java -jar ssecls.jar --api 2 --digitallysigned 1 --sha256 63ac0ad9c9dbeffdb4dc07c3c685dce4d41a4169eb5efabf9347dd577d3270d --md5hash 62825AA34568DA314E60D2AC2ACD2181 --sourceip "192.172.1.8" --sourceurl "www.symantec.com" --reportinsightinfo 1 --aggressionlevel 2 -f c:\testfolder\test.exe

See “Supported command-line options for Java based command-line scanner” on page 356.

See “Java based command-line scanner syntax and usage” on page 355.
About editing configuration data

This appendix includes the following topics:

- About editing the Symantec Protection Engine configuration files
- About configuration options

### About editing the Symantec Protection Engine configuration files

You can configure most of the options for Symantec Protection Engine through the Web-based console. However, there are configuration options that are not available in the console that you might need to reconfigure.

See “Before you install Symantec Protection Engine” on page 29.

You can change certain Symantec Protection Engine settings by modifying the data in the XML files.

The XML files that you can modify are as follows:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>configuration.xml</td>
<td>Contains logging, the temporary directory location, protocol configurations, and operating-system-specific settings</td>
</tr>
<tr>
<td>filtering.xml</td>
<td>Contains settings for URL filtering, MIME, and container limits</td>
</tr>
<tr>
<td>liveupdate.xml</td>
<td>Contains LiveUpdate options</td>
</tr>
<tr>
<td>policy.xml</td>
<td>Contains access-denied and notification messages, extension policy and extension lists, and Bloodhound scanning settings</td>
</tr>
</tbody>
</table>
Note: When you edit the configuration data, all high-ASCII and double-byte characters must be written in UTF-8 encoding.

When you are finished with editing the settings in the XML files, you must stop and restart Symantec Protection Engine. Changes to settings in the console (if any) appear the next time that you open the console.

See “Verifying, stopping, and restarting the Symantec Protection Engine daemon on Linux” on page 61.

See “Verifying, stopping, and restarting the Symantec Protection Engine service on Windows” on page 62.

Warning: Several configuration options are not addressed here and should not be changed. Changes to certain options can detrimentally affect product performance. For example, the installation directory is specified at installation, and the product does not function if you change this value.

About configuration options

To modify an XML file, you must know the XPath and the field values.

You can use the XML modifier command-line tool of Symantec Protection Engine to configure the following options:

- Configure the ICAP response in Symantec Protection Engine
  See “Configure the ICAP response” on page 368.

- Configure the ICAP preview option in Symantec Protection Engine
  See “Configure the ICAP preview option” on page 369.

- Control the dynamic thread pool
  See “Control the dynamic thread pool” on page 369.

- Disable the ICAP threshold client notification feature in Symantec Protection Engine
  See “Disable the ICAP threshold client notification” on page 372.

- Specify the maximum file name lengths in Symantec Protection Engine

- Configure the number of LiveUpdate retries in Symantec Protection Engine
  See “Configure the number of LiveUpdate retries” on page 372.

- Change the LiveUpdate base time
  See “Change the LiveUpdate base time” on page 373.

- Configure the LiveUpdate server details
See “Configure the LiveUpdate server details” on page 373.

- Extract all streams from OLE-structured storage documents for scanning
  See “Extract all streams from OLE structured storage documents for scanning” on page 375.

- Specify a replacement file name in Symantec Protection Engine
  See “Specify a replacement file name” on page 376.

- Specify archive file types to scan in Symantec Protection Engine
  See “Specify archive file types to scan” on page 376.

- Modify the ICAP options attribute-list extension in Symantec Protection Engine
  See “Modify the ICAP options attribute-list extension” on page 377.

- Modify the ICAP response to send the nonviral threat category name
  See “Modify the ICAP response to send the nonviral threat category name” on page 377.

- Access scan error files in Symantec Protection Engine
  See “Access scan error files” on page 378.

- Delete or repair infected read-only files in Symantec Protection Engine
  See “Delete or repair infected read-only files” on page 378.

- Enable nonviral threat categories information in Symantec Protection Engine
  See “Enable nonviral threat categories information” on page 380.

- Specify decomposer file size limit in Symantec Protection Engine
  See “Specify decomposer file size limit” on page 381.

- Specify maximum file size for extracted files in Symantec Protection Engine
  See “Specify maximum file size for extracted files” on page 381.

- Specify maximum cumulative file size for extracted files in Symantec Protection Engine
  See “Specify maximum cumulative file size for extracted files” on page 382.

- Specify maximum socket timeout value in Symantec Protection Engine
  See “Specify the maximum socket timeout value” on page 382.

- Change authentication mode settings for accessing Symantec Protection Engine console
  See “Change authentication mode settings for accessing Symantec Protection Engine console” on page 383.

- Add or change authorized security group name to access Symantec Protection Engine console
  See “Add or change authorized group name to access Symantec Protection Engine console” on page 383.
Configure the ICAP response

If your client uses ICAP, you can configure the ICAP response option.

You might need to adjust this setting depending on the ICAP 1.0 application for which Symantec Protection Engine provides scan and repair services. The default setting is to send an "access denied" message when a file is blocked because it is unrepairable. However, some ICAP 1.0 applications are configured to receive the ICAP 403 response instead.

Table C-1 lists the ICAP response settings.
Configure the ICAP preview option

The ICAP preview option specifies whether to send the transfer headers based on the extension list or to send a header to preview all.

Table C-2 lists the ICAP preview settings.

<table>
<thead>
<tr>
<th>XPath</th>
<th>Field values</th>
<th>Default setting</th>
</tr>
</thead>
</table>
| /configuration/ProtocolSettings/ICAP/ICAPPreviewAll/@value | ■ False
Send the transfer headers based on the Symantec Protection Engine extension lists.
■ True
Send a transfer-preview header indicating preview all.                      | True                                                                         |

See “About configuration options” on page 366.

Control the dynamic thread pool

The pool of scanning threads that is available to Symantec Protection Engine for antivirus scanning dynamically adjusts to the load that is processed. You can change several parameters to control the dynamic thread pool.
**Note:** To disable dynamic thread pool management and use a fixed thread pool size, use the same number of scanning threads that you set for the fixed thread pool for both the MinThreads and MaxThreads parameters. You must configure the maximum threads in the console.

The configuration file parameters for controlling the dynamic thread pool are as follows:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MinThreads</td>
<td>The minimum number of scanning threads that is created at startup time and the minimum to keep alive regardless of the load that is processed. The default settings depends on the number of cores of the processor.</td>
</tr>
<tr>
<td>GrowThreadCount</td>
<td>The GrowThreadCount is number of scanning threads to add when the existing threads cannot handle the load that is processed. The default setting is 4. The GrowThreadCount value must be larger than the ShrinkThreadCount value. Reasonable values are in the range of 0 to 16.</td>
</tr>
<tr>
<td>ShrinkThreadCount</td>
<td>The number of scanning threads to remove when more threads are running than are needed for the load that is processed. The default setting is 2. The ShrinkThreadCount value must be smaller than the GrowThreadCount value.</td>
</tr>
</tbody>
</table>

See “About available threads for scanning” on page 165.

The MinThreads value cannot be greater than the MaxThreads value. (Symantec Protection Engine does not validate the value that you input to ensure that it is lower than the MinThreads value.) If the MinThreads value is greater than MaxThreads value, Symantec Protection Engine generates the minimum thread pool based on the MinThreads value, regardless of MaxThreads value. As a result, the “Active threads” value and the ”Waiting threads” value on the Reports > Resources page would be greater than ”Thread pool size” value.

**Note:** You consume resources when you create new threads. After you create threads (GrowThreadCount), only make modifications when necessary. Remove threads (ShrinkThreadCount) more slowly than you add threads. In this way, you do not consume additional resources such as happens when you create new threads in a short period of time.
BusyRequestCount: The number of queued requests to be processed by scanning threads, which triggers the creation of more scanning threads.

The default setting is 4. The BusyRequestCount value cannot be less than 2.

IdleThreadCount: The number of idle scanning threads, which triggers the removal of scanning threads.

The default setting is 6.

SecondsBetweenChecks: The number of seconds between evaluations of the thread pool activity.

The default setting is 5 seconds. This value cannot be smaller than 2.

**Note:** Because thread pool activity is checked at the frequency that is specified for the SecondsBetweenChecks parameter, changes to the thread pool size occur at the same frequency.

Table C-3 lists the dynamic thread pool settings.

<table>
<thead>
<tr>
<th>XPath</th>
<th>Field values</th>
<th>Default setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>/configuration/Resources/System/MinThreads/@value</td>
<td>Integer between 0 - 512</td>
<td>Depends on the number of cores of the processor.</td>
</tr>
<tr>
<td>/configuration/Resources/System/GrowThreadCount/@value</td>
<td>Integer between 0 - 16</td>
<td>4</td>
</tr>
<tr>
<td>/configuration/Resources/System/ShrinkThreadCount/@value</td>
<td>Integer between 0 - 16</td>
<td>2</td>
</tr>
<tr>
<td>/configuration/Resources/System/BusyRequestCount/@value</td>
<td>Integer 0 or greater</td>
<td>4</td>
</tr>
<tr>
<td>/configuration/Resources/System/IdleThreadCount/@value</td>
<td>Integer between 0 - 16</td>
<td>6</td>
</tr>
<tr>
<td>/configuration/Resources/System/SecondsBetweenChecks/@value</td>
<td>Integer 2 or greater</td>
<td>5</td>
</tr>
</tbody>
</table>

See “About configuration options” on page 366.
Disable the ICAP threshold client notification

Symantec Protection Engine sends a notification to the specified logging destinations when it reaches scan queued requests threshold. If your client uses ICAP, Symantec Protection Engine also rejects the scan request and sends a notification to the client. This feature lets the client determine load balancing and prevents the server from being overloaded with scan requests.

If you disable the client notification feature, Symantec Protection Engine continues to send messages to the specified logging destinations when the threshold is met. The "Log or send alert for maximum load every <n> minutes" setting applies only to SMTP alerts.

Note: For logging to occur at maximum load, the logging level for the logging destination must be set to Warning or higher.

See “Allocating resources for Symantec Protection Engine” on page 81.
See “ICAP return codes” on page 393.
See “Logging levels and events” on page 202.
Table C-4 lists the threshold client notification settings.

<table>
<thead>
<tr>
<th>XPath</th>
<th>Field values</th>
<th>Default setting</th>
</tr>
</thead>
</table>
| /configuration/ProtocolSettings/EnableServerTooBusyResponse @value | ■ False  
Disables the ICAP threshold client notification.  
■ True  
Enables the ICAP threshold client notification. | True             |

See “About configuration options” on page 366.

Configure the number of LiveUpdate retries

You can schedule LiveUpdate to run automatically by using the Symantec Protection Engine console. Scheduling LiveUpdate to occur automatically at a specified time interval ensures that Symantec Protection Engine always has the most current virus and URL definitions.

See “Configuring LiveUpdate to occur automatically” on page 230.
If LiveUpdate fails, you can configure the number of times Symantec Protection Engine should continue to try to perform a content LiveUpdate. Table C-5 lists the LiveUpdate retry settings.

Table C-5  LiveUpdate retry settings

<table>
<thead>
<tr>
<th>XPath</th>
<th>Field values</th>
<th>Default setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>/liveupdate/Schedule/Retries/@value</td>
<td>Integer 0 or greater</td>
<td>4</td>
</tr>
</tbody>
</table>

See “About configuration options” on page 366.

Change the LiveUpdate base time

You can change the relative start time (or LiveUpdate base time) from which to calculate scheduled LiveUpdate tries. If you change the LiveUpdate base time, the LiveUpdate tries are scheduled every LiveUpdateSchedule seconds after the base time. The default LiveUpdate base time is the time at which Symantec Protection Engine was installed.

See “Configuring LiveUpdate to occur automatically” on page 230.

The LiveUpdate base time is specified in UTC seconds since 00:00:00 January 1, 1970.

Table C-6 lists the LiveUpdate base time settings.

Table C-6  LiveUpdate base time settings

<table>
<thead>
<tr>
<th>XPath</th>
<th>Field values</th>
<th>Default setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>/liveupdate/Schedule/BaseTime/@value</td>
<td>Integer 0 or greater</td>
<td>&lt;install time&gt;</td>
</tr>
</tbody>
</table>

See “About configuration options” on page 366.

Configure the LiveUpdate server details

You are asked to enter the LiveUpdate server details only in case of an upgrade with preserve settings option. However, you can change the values of the LiveUpdate server after the installation. In case of a fresh install or a clean upgrade, the LiveUpdate server details in the liveupdate.xml file will be the same as the details in the liveupdate.xml file shipped in the installer.

After a preserve settings upgrade, the liveupdate.xml file will contain some of the required settings that you set during the installation or in the form of silent parameters
in case of a silent installation. You can set the following parameters at the time of installation:

- Server Name
- Server Port
- Server Path
- Server Proxy Name
- Server Proxy Port

See "Creating the response file" on page 326.

See “About implementing a silent installation for Windows” on page 331.

Table C-7 lists the LiveUpdate server parameters.

<table>
<thead>
<tr>
<th>XPath</th>
<th>Field values</th>
<th>Default values</th>
</tr>
</thead>
<tbody>
<tr>
<td>/liveupdate/UpdateServer/Protocol/@value</td>
<td>http</td>
<td>http</td>
</tr>
<tr>
<td>/liveupdate/UpdateServer/Server/@value</td>
<td>The server name or IP address</td>
<td>liveupdate.symantec.com</td>
</tr>
<tr>
<td>/liveupdate/UpdateServer/Port/@value</td>
<td>Integer from 0 through 65535</td>
<td>80</td>
</tr>
<tr>
<td>/liveupdate/UpdateServer/Path/@value</td>
<td>The directory on the LiveUpdate server that contains the LiveUpdate packages</td>
<td>NA</td>
</tr>
<tr>
<td>/liveupdate/UpdateServer/UserName/@value</td>
<td>The user name to log on to the LiveUpdate server</td>
<td>NA</td>
</tr>
<tr>
<td>/liveupdate/UpdateServer/Password/@value</td>
<td>The password to log on to the LiveUpdate server</td>
<td>NA</td>
</tr>
</tbody>
</table>

Table C-8 lists the LiveUpdate proxy server parameters.
### Table C-8  Proxy server parameters

<table>
<thead>
<tr>
<th>XPath</th>
<th>Field values</th>
<th>Default values</th>
</tr>
</thead>
<tbody>
<tr>
<td>/configuration/ProxyServerSettings/ServerName/@value</td>
<td>The proxy server name or IP address</td>
<td>NA</td>
</tr>
<tr>
<td>/configuration/ProxyServerSettings/ServerPort/@value</td>
<td>Integer from 0 through 65535</td>
<td>0</td>
</tr>
<tr>
<td>/configuration/ProxyServerSettings/UserName/@value</td>
<td>The user name to log on to the proxy server</td>
<td>NA</td>
</tr>
<tr>
<td>/configuration/ProxyServerSettings/Password/@value</td>
<td>The password to log on to the proxy server</td>
<td>NA</td>
</tr>
</tbody>
</table>

**Note:** If you change any of the values related to the LiveUpdate server in the `liveupdate.xml` file, you will need to restart the Symantec Protection Engine service.

### Extract all streams from OLE structured storage documents for scanning

Certain Microsoft files (such as Microsoft Word and Excel documents) are object linking and embedding (OLE) structured storage documents. OLE is a compound document standard developed by Microsoft. It enables objects to be created with one application and linked or embedded in a second application. In this type of structured storage document, data is stored in a number of streams. Only certain streams typically contain the content that can contain viruses. Symantec Protection Engine is configured by default to extract and scan all streams. Performance might be adversely affected depending on the number (and content) of files to be scanned.

Table C-9 lists the OLE-structured storage document scanning settings.

### Table C-9  OLE-structured storage document scanning settings

<table>
<thead>
<tr>
<th>XPath</th>
<th>Field values</th>
<th>Default setting</th>
</tr>
</thead>
</table>
| /filtering/Container/Options/ExtractNativeOLEStreamsOnly/ @value | ■ False  
Extracts all streams.  
■ True  
Extracts only the native OLE streams. | False |

See “About configuration options” on page 366.
Specify a replacement file name

Use this option to specify the name of the attachment file that is returned when Symantec Protection Engine deletes a file. The replacement file contains a message that indicates the name of the deleted file and why it was deleted.

Table C-10 lists the replacement file name settings.

Table C-10 Replacement file name settings

<table>
<thead>
<tr>
<th>XPath</th>
<th>Field values</th>
<th>Default setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>/filtering/Container/ReplacementFilename/@value</td>
<td>Any valid file name.</td>
<td>DELETE%.TXT</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The percentage mark (%) is a sequence number. For example, if two attachments are deleted, the replacement files are called DELETE0.TXT and DELETE1.TXT.</td>
</tr>
</tbody>
</table>

See “About configuration options” on page 366.

Specify archive file types to scan

You can specify the types of archive files for which Symantec Protection Engine extracts (decompresses) and scans the internal files.

Note: If the list is empty, Symantec Protection Engine does not scan any archive files.

Table C-11 lists the archive file types to scan settings.

Table C-11 Archive file types to scan settings

<table>
<thead>
<tr>
<th>XPath</th>
<th>Field values</th>
<th>Default setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>/filtering/Container/DecEngines</td>
<td>amg, arj, cab, gzip, 7z, id, lha, lz, ole1, ss, rar, rtf, tar, tnef, zip, text, mb3, as, bzip2, pdf, mms, ace</td>
<td>zip, ss, gzip, cab, lha, tnef, arj, rar, lz, amg, tar, rtf, bzip2, pdf, 7z, mms, ole1, ace, mb3, as, text</td>
</tr>
</tbody>
</table>

See “About configuration options” on page 366.
Modify the ICAP options attribute-list extension

To list all of the categories that are available for URL filtering, Symantec Protection Engine uses the Attribute-List response body extension in a response to an ICAP OPTIONS request. This extension is formally specified in the ICAP Extensions Internet Draft, section 5.2.

To use this extension, an OPTIONS response must specify the header Encapsulated:opt-body=0. Not all ICAP clients recognize the opt-body encapsulation, so Symantec Protection Engine makes the opt-body and Attribute-List optional. However, they are included by default.

To make it possible to disable their use, the OptBodyAllowed option is included in the configuration settings. If the OptBodyAllowed value is set to true (the default setting), then Attribute-List is included in OPTIONS responses. If the OptBodyAllowed value is set to false, then Attribute-List is not included in OPTIONS responses. If OptBodyAllowed is set to false, an ICAP client that wants to use the URL filtering in audit mode cannot obtain the list of filtering categories that are available.

Table C-12 lists the OptBodyAllowed header settings.

**Table C-12** OptBodyAllowed header settings

<table>
<thead>
<tr>
<th>XPath</th>
<th>Field values</th>
<th>Default setting</th>
</tr>
</thead>
</table>
| /configuration/protocol/ICAP/OptBodyAllowed/@value | ▪ True  
                      Returns the list of categories.  
▪ False  
                      Does not return a list of categories. | True            |

See “About configuration options” on page 366.

Modify the ICAP response to send the nonviral threat category name

You can specify whether you want ICAP to return the name of the nonviral threat in its response when such a threat is detected. By default, the ICAP response does not send the nonviral threat category name.

Table C-16 lists the EnableNonViralThreatCategoryResp header settings.

See “About configuration options” on page 366.
Access scan error files

By default, Symantec Protection Engine blocks files that produce an Internal Server Error. You can modify the AllowAccessOnScanError command to permit access to these files.

When you enable this setting, a Warning level log event is generated each time access is permitted to files that produced an Internal Server Error. This log event is sent to all logging destinations except SNMP.

This command applies to the ICAP protocols and RPC protocols only. For ICAP, the client must permit the Allow: 204 ICAP header return code with the request.

Table C-13 lists the AllowAccessOnScanError settings.

<table>
<thead>
<tr>
<th>XPath</th>
<th>Field values</th>
<th>Default setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>/policies/ThreatPolicies/Actions/</td>
<td></td>
<td>False</td>
</tr>
<tr>
<td>AllowAccessOnScanError</td>
<td>False Prohibits an access to the files that are blocked by the Internal Server Error result.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>True Permits an access to the files that are normally blocked by the Internal Server Error result.</td>
<td></td>
</tr>
</tbody>
</table>

See “About configuration options” on page 366.

Delete or repair infected read-only files

Symantec Protection Engine can scan the files that are marked read-only but cannot repair or delete them if the scanning policy is to repair or delete. You can modify the HonorReadOnly command to overwrite the read-only setting so that Symantec Protection Engine can repair or delete infected read-only files. This command applies to all protocols on the Windows platform.

Table C-15 lists the HonorReadOnly settings.
Table C-14  HonorReadOnly settings

<table>
<thead>
<tr>
<th>XPath</th>
<th>Field values</th>
<th>Default setting</th>
</tr>
</thead>
</table>
| /policies/ThreatPolicies/Actions/HonorReadOnly/@value | ■ False  
  Symantec Protection Engine repairs or deletes the read-only file, if that is the scanning policy.  
  ■ True  
  Symantec Protection Engine does not repair or delete the read-only file, even if that is the scanning policy. | True            |

See “About configuration options” on page 366.

Disable automatic self-test scanning

If your client uses the ICAP protocol or the RPC protocol, Symantec Protection Engine installs with a self-test scanning feature. Symantec Protection Engine performs a test every minute to check whether it is responsive and able to scan files. A test file is sent for Symantec Protection Engine to scan. If Symantec Protection Engine does not respond with a scan result before the timeout period expires, a Warning message is logged. Each self-test scan occurs 1 minute after the last self-test scan finishes.

Disable this feature if any of the following conditions apply:

■ You do not want the automatic self-testing scanning events to be logged to the specified logging destinations.

■ You configure Symantec Protection Engine to send alerts for Warning level events, but you do not want alerts about this event.

See “Logging levels and events” on page 202.

Table C-15 lists the selfscantest settings.

Table C-15  selfscantest settings

<table>
<thead>
<tr>
<th>XPath</th>
<th>Field values</th>
<th>Default setting</th>
</tr>
</thead>
</table>
| /configuration/Miscellaneous/SelfScanTest/@enabled | ■ True  
  Self-scan testing is enabled.  
  ■ False  
  Self-scan testing is disabled. | True            |

See “About configuration options” on page 366.
Enable nonviral threat categories information

The ICAP response headers that Symantec Protection Engine uses indicate the total number of violations that are found in the scanned data. If violations are detected, a series of indented lines that contain information about each violation follow the header.

By default, Symantec Protection Engine does not send the threat category name in the ICAP response header. However, you can modify the EnableNonViralThreatCategoryResp value to include the threat category name in the header.

When enabled, the field in the response header appears as "ThreatDescription" and contains the threat category name. The threat category name is appended to the virus name with a delimiter pipe; for example, ThreatDescription = <VirusName>|NonViralThreat=<CategoryName>.

After you modify the default setting using the command-line tool, restart the Symantec Protection Engine service.

See “Verifying, stopping, and restarting the Symantec Protection Engine daemon on Linux” on page 61.

See “Verifying, stopping, and restarting the Symantec Protection Engine service on Windows” on page 62.

For more information about ICAP response headers, see the Symantec Protection Engine Software Developer's Guide.

Table C-16 lists the EnableNonViralThreatCategoryResp settings.

**Table C-16** EnableNonViralThreatCategoryResp settings

<table>
<thead>
<tr>
<th>XPath</th>
<th>Field values</th>
<th>Default setting</th>
</tr>
</thead>
</table>
| /configuration/ProtocolSettings/ICAP/EnableNonViralThreatCategoryResp/@value | ■ True  
Symantec Protection Engine sends the nonviral threat category name.  
■ False  
Symantec Protection Engine does not send the nonviral threat category name. | False |

See “About configuration options” on page 366.
Specify decomposer file size limit

Use this parameter to specify the maximum top level container file size that the decomposer can process. The decomposer does not process any top level container file of size equal to or greater than the value that you specify in Symantec Protection Engine. The DecFileSize parameter accepts a value in GB. The maximum top-level container file size that you can specify in Symantec Protection Engine for tar, rar, and zip containers is 30GB (approximately 30719 MB). For other containers, you can specify a maximum top-level container file size of 2 GB (approximately 1907 MB).

For example, if you specify 20 GB as the maximum limit, then the decomposer processes a top-level container file of type tar/rar/zip of size less than 20 GB. For any other top level container file type, the limit is still 2 GB.

Table C-17 lists the decomposer file size limit settings.

<table>
<thead>
<tr>
<th>XPath</th>
<th>Field values</th>
<th>Default setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>/filtering/Container/DecFileSize/@value</td>
<td>Integer 1 through 30</td>
<td>30</td>
</tr>
<tr>
<td></td>
<td>Type 0 to disable this setting</td>
<td></td>
</tr>
</tbody>
</table>

Note: This parameter does not limit the size of individual files that are extracted from the top level container file.

See “About configuration options” on page 366.

Specify maximum file size for extracted files

Use this parameter to specify maximum file size for the individual files that can be extracted on disk and in memory in Symantec Protection Engine. The MaxExtractSize parameter accepts a value in MB. The maximum extract file size that you can specify for individual files in tar, rar, and zip containers is 30719 MB (approximately 30 GB). For other containers, you can specify a maximum extract file size of 1907 MB (approximately 2 GB) for its individual files.

For example, if you specify 20480 MB as the maximum limit, then the decomposer can extract individual files each of size up to 20480 MB from top level container file of type tar, rar, and zip. For any other top level container file type, the limit is still 1907 MB.

Table C-18 lists the extracted file size settings
### Specify maximum cumulative file size for extracted files

Use this parameter to specify the maximum cumulative file size for extracted files. Symantec Protection Engine calculates the cumulative file size after each file is extracted. This parameter stops the recursive scanning of individual files once this file size limit is reached. Once the maximum limit is reached, the remaining files in the container are not extracted. The MaxCumulativeExtractSize parameter accepts a value in bytes. The maximum limit you can enter is 32212254720 bytes (approximately 30 GB). A value of zero (0) disables this optimization setting.

Table C-19 lists the settings to configure maximum cumulative file size for extracted files.

#### Table C-19 Maximum cumulative file size for extracted files

<table>
<thead>
<tr>
<th>XPath</th>
<th>Field values</th>
<th>Default setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>/filtering/Container/MaxCumulativeExtractSize/@value</td>
<td>Accepts a value in bytes Type 0 to disable this setting</td>
<td>0</td>
</tr>
</tbody>
</table>

See “About configuration options” on page 366.

### Specify the maximum socket timeout value

Typically, a client sends a file to Symantec Protection Engine to scan over a socket and Symantec Protection Engine returns a response after it is scanned over the same socket. The total time to send the file and receive the response depends upon the file size. The larger the file, the longer Symantec Protection Engine takes to decompose and scan the file. So it takes longer for the response to reach the client. If you specify a small value for socket timeout, a socket timeout error gets generated. You can specify a larger socket timeout value to avoid the socket timeout error.

The maximum socket timeout value that you can enter is 4320 minutes (72 hours) while the default value is 5 minutes.
Table C-20 lists the maximum socket timeout value.

<table>
<thead>
<tr>
<th>XPath</th>
<th>Field values</th>
<th>Default setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>/configuration/Resources/System/SocketTimeOut/@value</td>
<td>Accepts a value in minutes</td>
<td>5</td>
</tr>
</tbody>
</table>

See “About configuration options” on page 366.

Change authentication mode settings for accessing Symantec Protection Engine console

Use this option to select the authentication mode for accessing the Symantec Protection Engine console.

<table>
<thead>
<tr>
<th>XPath</th>
<th>Field values</th>
<th>Default setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>//Resources/System/admin/ADAuthenticationMode/@value</td>
<td>■ True Enables Windows Active Directory-based authentication mode. ■ False Enables Symantec Protection Engine-based authentication</td>
<td>The default setting is based on the authentication mode that is selected during installation. During silent installation if authentication mode is not specified, then the default value is set to false.</td>
</tr>
</tbody>
</table>

See “About installing Symantec Protection Engine” on page 35.
See “About configuration options” on page 366.

Add or change authorized group name to access Symantec Protection Engine console

This option is valid only for Windows Active Directory-based authentication mode where users from the specified domain\groupname are allowed access to the Symantec Protection Engine console.

For more information on how to change authentication modes, see Change authentication mode settings for accessing Symantec Protection Engine console
Table C-22  To change authorized group name

<table>
<thead>
<tr>
<th>XPath</th>
<th>Field values</th>
<th>Default setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>//Resources/System/admin/ADAuthenticationMode/</td>
<td>Any valid domain and group name in the format domain\groupname.</td>
<td>None</td>
</tr>
<tr>
<td>ActiveDirectoryDetails/@groupname</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

See “About configuration options” on page 366.

Add RPC clients

Use this option to add a network attached storage device to the RPC client list. This option accepts the IP address of a single network attached storage device. To add more than one device, you must use this option multiple times. You must use the "-c" switch of the XML modifier to add a network attached storage device.

Table C-23  Add network attached storage device settings

<table>
<thead>
<tr>
<th>XPath</th>
<th>Field values</th>
<th>Default setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>//configuration/ProtocolSettings/RPC/ClientList/items</td>
<td>IP address of RPC Client /NAS Device</td>
<td>None</td>
</tr>
</tbody>
</table>

See “About configuration options” on page 366.

Configure MS Office file scanning

Use this option to configure Symantec Protection Engine to enhance scanning of MS Office files.

Table C-24 lists MS Office file scanning option settings.

Table C-24  MS Office file scanning settings

<table>
<thead>
<tr>
<th>XPath</th>
<th>Field values</th>
<th>Default setting</th>
</tr>
</thead>
</table>
| /filtering/Container/EnableMSOfficeCRD/@value               | ■ True
MS Office file scanning option is enabled
■ False
MS Office file scanning option is disabled                  | True                                                                       |

See “About configuration options” on page 366.
Specify file size threshold for scanning exclusion

Use this parameter to specify the file size that can be excluded from scanning. The files greater than or equal to the specified value are not scanned. Symantec Protection Engine reports the file as clean and sends an ICAP response code 200 OK. It also logs that the file was bypassed from scanning and the number of requests are incremented by 1. The \texttt{FileSizeScanThreshold} parameter is supported in ICAP FILEMOD and RPC protocol only. The \texttt{FileSizeScanThreshold} parameter accepts values in bytes.

<table>
<thead>
<tr>
<th>XPath</th>
<th>Field values</th>
<th>Default setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>/filtering/FileAttribute/</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FileSizeScanThreshold/@value</td>
<td>Integer 0 or greater</td>
<td>0</td>
</tr>
</tbody>
</table>

See “About configuration options” on page 366.

Specify file size threshold for in-place scanning

This parameter is applicable in RPC protocol only. Scanning files over the network can cause network congestion. You can choose to scan files in-place on the RPC client share, thus improving the overall performance.

The \texttt{FilerPerformanceThreshold} parameter allows you to specify the file size threshold value below which the file is copied from the RPC client share to the Protection Engine temporary folder. Hence, to ensure that most of the files are scanned in-place, you must enter a threshold value lesser than the average file size in your environment.

The \texttt{FilerPerformanceThreshold} parameter accepts value in bytes. If you specify the default value (0) then all files are copied to Protection Engine temporary folder and then scanned.

<table>
<thead>
<tr>
<th>XPath</th>
<th>Field values</th>
<th>Default setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>/configuration/ProtocolSettings/</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RPC/FilerPerformanceThreshold/ @value</td>
<td>Integer 0 or greater</td>
<td>0</td>
</tr>
</tbody>
</table>

See “About configuration options” on page 366.
Include category information from ICAP response in URL filtering

Use this option to include category information from ICAP response when URL is scanned.

Table C-27  EnableCategoryTypeInICAPResponse settings

<table>
<thead>
<tr>
<th>XPath</th>
<th>Field values</th>
<th>Default setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>/configuration/ProtocolSettings/ICAP/EnableURLCategoryTypeInICAPResponse/@value</td>
<td>■ True category information (Local / Vendor) is present in ICAP response when URL is scanned. &lt;br&gt; ■ False Category information is not present in ICAP response when URL is scanned.</td>
<td>False</td>
</tr>
</tbody>
</table>

Enable subcategories description

The ICAP response headers that Symantec Protection Engine uses indicate the total number of violations that are found in the scanned data. If violations are detected, a series of indented lines that contain information about each violation follow the header.

Each detected viral or nonviral threat has an uber category and subcategory associated with it. The subcategory description provides more information about a subcategory. By default, Symantec Protection Engine does not send the subcategory description in the ICAP response. However, the user can get this information by enabling EnableSubCategoryDescriptionResp.

Table C-28  EnableSubCategoryDescriptionResp settings

<table>
<thead>
<tr>
<th>XPath</th>
<th>Field values</th>
<th>Default setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>/configuration/ProtocolSettings/ICAP/EnableSubCategoryDescriptionResp/@value</td>
<td>■ True Symantec Protection Engine sends the subcategory description. &lt;br&gt; ■ False Symantec Protection Engine does not send subcategory description.</td>
<td>False</td>
</tr>
</tbody>
</table>
Enable threat categories information

The ICAP response headers that Symantec Protection Engine uses indicate the total number of violations that are found in the scanned data. If violations are detected, a series of indented lines that contain information about each violation follow the header.

By default, Symantec Protection Engine does not send the threat category name in the ICAP response header. However, you can modify the EnableThreatCategoryResp value to include the threat category name in the header.

When enabled, the field in the response header appears as "ThreatDescription" and contains the threat category name. The threat category name is appended to the virus name with a delimiter pipe; for example, ThreatDescription = <VirusName>|NonViral Threat=<CategoryName>.

After you modify the default setting using the command-line tool, restart the Symantec Protection Engine service.

<table>
<thead>
<tr>
<th>XPath</th>
<th>Field values</th>
<th>Default values</th>
</tr>
</thead>
</table>
| /configuration/ProtocolSettings/ICAP/EnableThreatCategoryInformation/@value | True  
Symantec Protection Engine sends the threat category name.  
False  
Symantec Protection Engine does not send the threat category name. | True |

Note: This parameter is only applicable with new ICAP services introduced in Symantec Protection Engine version 7.0 and later. For more information, see the *Symantec Protection Engine Software Developer’s Guide*. 

| Note: This parameter is only applicable with new ICAP services introduced in Symantec Protection Engine version 7.0 and later. For more information, see the *Symantec Protection Engine Software Developer’s Guide*. 

| Note: This parameter is only applicable with new ICAP services introduced in Symantec Protection Engine version 7.0 and later. For more information, see the *Symantec Protection Engine Software Developer’s Guide*. |
Specify file path exclusion for scanning in Symantec Protection Engine

You can select the files to be excluded from scanning by specifying the file path. Symantec Protection Engine excludes files from scanning based on the location of the files.

**Note:** A maximum of 32 file paths can be excluded from scanning.

Table C-30 lists the file path exclusion scanning settings.

<table>
<thead>
<tr>
<th>XPath</th>
<th>Field value</th>
<th>Default setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>/filtering/FileAttribute/DenyFilePaths/items/item/@value</td>
<td>A valid field value. <strong>Note:</strong> The file path is case sensitive and each file path must be at a separate line.</td>
<td>None</td>
</tr>
</tbody>
</table>

To add an exclusion file path

1. Create a .txt file with the list of file paths to be used by Symantec Protection Engine that are to be excluded from scanning.

   **Note:** The file paths are case sensitive and each file path must be at a new line.

   Also, the file paths must be unique. The xmlmodifier command does not check for duplicate file path entries.

2. Save the file to your system.

3. Run the following command:

   ```sh
exmlmodifier -b //filtering/FileAttribute/DenyFilePaths <Path of a text file containing list of exclude file> filtering.xml
   
   For example: C:\Program Files\Symantec\Scan Engine> xmlmodifier -b //filtering/FileAttribute/DenyFilePaths F:\Path_list.txt filtering.xml
   
   where F:\Path_list.txt contains the following file paths:
   - C:\testfiles\
   ```
F:\test\n\10.217.1.2\ONTAP_ADMIN$\vol\vol0\home\test\abc\n
Note: The file path can include the name of the file too. For example, C:\testfiles\abc.txt, which means that only the abc.txt file in the testfiles folder is excluded from scanning.

4 Restart the Symantec Protection Engine service.

To manually modify/delete an exclusion file path
1 Open the filtering.xml file and manually delete the file path that needs to be modified.
2 Save the file.
3 Add the new file path to the .txt file, and save the file.

Note: The file paths must be unique. The xmlmodifier command does not check for duplicate file path entries.

4 Run the following command:
xmlmodifier -b //filtering/FileAttribute/DenyFilePaths <Path of a text file containing list of exclude file> filtering.xml

5 Restart the Symantec Protection Engine service.

To modify/delete an exclusion file path using the xmlmodifier command
1 Run the following command:
xmlmodifier -r //filtering/FileAttribute/DenyFilePaths/items filtering.xml

Note: This command removes all the file paths.

2 Add the new file paths to the .txt file, and save the file.

Note: The file paths must be unique. The xmlmodifier command does not check for duplicate file path entries.
3 Run the following command:

```bash
xmlmodifier -b //filtering/FileAttribute/DenyFilePaths <Path of a text file containing list of exclude file> filtering.xml
```

4 Restart the Symantec Protection Engine service.

See “About configuration options” on page 366.

Configure the additional parameters of APK Reputation

Apart from the basic APK Reputation configurations, you can configure the following parameters as per requirements:

- **Query timeout value**
  
  QueryTimeout is a timeout value that SPE server waits to get result from APK service in a cache.

- **Scan timeout value**
  
  ScanTimeout is a timeout value that SPE waits to get APK reputation result if it’s not available in a cache. If scan timeout is reached, SPE provides verdict based on antivirus scan.

  For example, **ScanTimeout value** is set to 10 seconds and **QueryTimeout value** is set to 20 seconds. For a particular APK file, if it takes more than 10 seconds for SPE to get the response from the APK Reputation server, it gives the **ICAP response APKResult=21** in X-APK-Reputation-Info header.

  In the backend, SPE continues to wait for response from the server. When SPE gets the response, it stores the same in APK cache. So, the next time if the same file is scanned, **APKResult=21** response will not be seen in ICAP response. SPE will give proper verdict for the file based on the response that it received earlier from APK reputation server.

- **Threshold cache entries value to be maintained**

- **Cache time to live value**
  
  This parameter sets the time for which cache entries to be maintained in cache. After the specified time limit the cache is emptied.

- **Save cache to the disc**

- **Time interval after which cache will be saved to the disc**

- **Minimum threads value**

- **Maximum threads value**

- **APK Reputation scanning based on file size**
### Table C-31  APK Reputation settings

<table>
<thead>
<tr>
<th>XPath</th>
<th>Field values</th>
<th>Default setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>/policies/ThreatPolicies/APKReputation/QueryTimeOut/@value</td>
<td>0 to 4294967295 seconds.</td>
<td>30 seconds</td>
</tr>
<tr>
<td>/policies/ThreatPolicies/APKReputation/ScanTimeOut/@value</td>
<td>0 to 2147483647 milliseconds</td>
<td>5000 milliseconds</td>
</tr>
<tr>
<td>/policies/ThreatPolicies/APKReputation/CacheSettings/ThresholdCacheEntries/@value</td>
<td>10 to 100000</td>
<td>10000</td>
</tr>
<tr>
<td>/policies/ThreatPolicies/APKReputation/CacheSettings/CacheTimeToLive/@value</td>
<td>0 with Cache time to live value will be based on APK file's security rating.</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>600 to 2592000 seconds</td>
<td></td>
</tr>
<tr>
<td>/policies/ThreatPolicies/APKReputation/CacheSettings/CacheDump/@enabled</td>
<td>true Enables saving cache to the disc. false Disables saving cache to the disc.</td>
<td>true</td>
</tr>
<tr>
<td></td>
<td>3600 to 432000 seconds</td>
<td>43200 seconds</td>
</tr>
<tr>
<td>/policies/ThreatPolicies/APKReputation/ThreadPool/MinThreads/@value</td>
<td>0 to 32</td>
<td>2</td>
</tr>
<tr>
<td>/policies/ThreatPolicies/APKReputation/ThreadPool/MaxThreads/@value</td>
<td>1 to 32</td>
<td>32</td>
</tr>
<tr>
<td>/policies/ThreatPolicies/APKReputation/FileSizeExclusionThreshold/@value</td>
<td>1 to 2147483647 bytes</td>
<td>102400000 bytes</td>
</tr>
</tbody>
</table>

See “About Android Application (APK) Reputation” on page 193.

### Configuring the additional parameters of URL Reputation

Apart from the basic URL Reputation configurations, you can configure the following parameters as per the requirements.

- Enable match exact URLs only option
- Configure the reputation level
- Configure the confidence level

<table>
<thead>
<tr>
<th>XPath</th>
<th>Field values</th>
<th>Default setting</th>
</tr>
</thead>
</table>
| /filtering/URLReputation/MatchExactURLsOnly/@value | ■ true Match Exact URLs Only parameter is enabled.  
■ false Match Exact URLs Only parameter is disabled. | true false      |
| /filtering/URLReputation/Threshold/@reputation <value> | ■ 1 to 10  | 8 |
| /filtering/URLReputation/Threshold/@confidence <value> | ■ 1 to 5 | 4 |
Return codes

This appendix includes the following topics:

- ICAP return codes
- RPC protocol return codes

ICAP return codes

The following return codes are generated for ICAP version 1.0:

- 100 Continue.
- 200 OK.
- 201 Created.
- 204 No content necessary.
- 400 Bad request.
- 403 Forbidden. Infected and not repaired.
- 404 Not found.
- 500 Internal server error.
- 502 Bad gateway.
- 505 ICAP version not supported.
- 506 Server too busy.
- 551 Resource unavailable.
- 558 Aborted - no scanning license.
RPC protocol return codes

The following return codes are generated for RPC:

- Infection found, repaired
- Infection found, repair failed
- Infection found, repair failed, file quarantined
- Infection found, repair failed, quarantine failed
- Infection found
- Maximum Extract Size exceeded, scan incomplete
- Maximum Extract Time exceeded, scan incomplete
- Maximum Extract Depth exceeded, scan incomplete
- Aborted - No AV scanning license
- Internal server error
- Infection found, repair failed, read-only file
- Malformed container found
- Error creating temporary file
- Error replacing infected file
- Internal server error (File access allowed)
- Encrypted container found
Common LiveUpdate error codes

This appendix includes the following topics:

- Common LiveUpdate error codes

Common LiveUpdate error codes

Table E-1 lists the most common LiveUpdate error codes and their description.

<table>
<thead>
<tr>
<th>Error code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>24</td>
<td>No update available post rollback unless the new set of definitions are available.</td>
</tr>
<tr>
<td>27</td>
<td>Update aborted. Timeout reached.</td>
</tr>
<tr>
<td>28</td>
<td>Update aborted. Download Failed.</td>
</tr>
<tr>
<td>29</td>
<td>Update aborted. Another LiveUpdate session is in progress.</td>
</tr>
<tr>
<td>30</td>
<td>Error connecting to update server.</td>
</tr>
<tr>
<td>31</td>
<td>Error while downloading specified component.</td>
</tr>
<tr>
<td>35</td>
<td>LiveUpdate session canceled.</td>
</tr>
<tr>
<td>41</td>
<td>Invalid product name while performing LiveUpdate.</td>
</tr>
<tr>
<td>42</td>
<td>LiveUpdate download and transport related errors.</td>
</tr>
<tr>
<td>48</td>
<td>LiveUpdate aborted due to low or no disk space.</td>
</tr>
<tr>
<td>Error code</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-------------</td>
</tr>
<tr>
<td>55</td>
<td>Server selection failed.</td>
</tr>
<tr>
<td>62</td>
<td>LiveUpdate is unable to find a valid license for requested feature update.</td>
</tr>
</tbody>
</table>
Symbols
.zip files. See container files

A
ActiveX 110
advanced heuristic scanning 117–118
adware
  nonviral threat 117
alerts 213
  See also logging
  about 213
  intervals, maximum load 81
  outbreak notifications 216
  SMTP 214
  SNMP 215
antivirus. See threats
auto-refresh 225

B
bind address
  ICAP 98
  log 205

C
certificate file 68
Certificate Import Utility 68
command-line scanner
  about 337
  file scanning 338
  installing 338
  IP address and port 346
  options 341
  recursive scanning 350
  redirecting console output 352
  scanning mode 347
  scanning results 347
  supported platforms 338
  supported protocol 338
  syntax and usage 339
  configuration data 365
  configuration.xml 365
  console 365
    See also XML modifier command-line tool
    accessing 65
    configuring interface settings 70
    port number 70
    server address 70
    SSL port number 70
    timeout 70
container files
  encrypted container file 134
  handling unscannable files 130
  malformed container file 132
  partial container files 131
  setting processing limits 161
content categories 182
  See also HTTP filtering
  See also local categories
content license 88
core server only mode 249
create new user accounts
  options 74
  process 74

D
DBCS path names 339
definitions
  about 226
  Rapid Release 243
  types 226
 updating
    using Intelligent Update package 237
    using LiveUpdate 229
delete user accounts
  options 78
  process 78
dynamic thread pool 81

E
edit user accounts
  options 76
edit user accounts  (continued)
process 76
email, filtering by
  file name 122
  file or attachment size 124
  maximum mail size 160
  message origin 128
  subject 126
events, logging 202

F
filtering. See HTTP filtering and email, filtering by
filtering.xml 365
fulfillment ID 93

H
home page
  auto-refresh 225
  scanning summary 222, 224
HTTP filtering
  about 168
  customizing the access denied message 190
  local categories 182
  modes 183
  URL categories 168
HTTPS server 67

I
ICAP
  about 97
  bind address 98
  command-line scanner, using 337
  configuring 98
  port number 98
  quarantining files 119
  return codes 393
  scan policy 98
  supported services 95
installation
  authentication modes 36
  command-line scanner 338
  on Linux 53, 56–57
  on Windows 37, 43–44
  preparing for 29
Intelligent Update  (continued)
  disabling 242
  enabling 240
  updating definitions 241

J
JRE (Java Runtime Environment) 29

K
keys 67
keystore 67

L
license
  content 93
  content license 88
  locating the serial number 90
  product 93
  product license 88
licensing
  about 88
  activating 90
  checking status 93
  license file
    installing 92
    obtaining 91
    removing 93
  types of licenses 88
Linux
  installing Symantec Protection Engine 53
  stopping and starting service 61
  uninstalling 87
  upgrading Symantec Protection Engine 56–57
LiveUpdate
  about 229
  configuring LiveUpdate server 232
  definitions, Symantec update frequency 227
  licensing requirement 88
  logs 233
  rolling back definitions 245
  updating definitions
    automatically 230
    on demand 231
LiveUpdate error codes 395
liveupdate.xml 365
load 149
load balancing 22
local categories 182
   See also content categories
   See also HTTP filtering
   about 182
   managing 185
local logging
   configuring 207
   exporting data 220
   managing local logs 218
   purging log files 210
   statistics reporting 211
   viewing data 219
logging 213
   See also alerts
   about 200
   changing log file location 208
   configuring local logging 207
   destinations 200
   levels and events 202
   outbreak alerting 216
   purging log files 210
   reporting functions 218
   SMTP alerts 214
   SNMP alerts 215
   statistics reporting 211
   viewing statistic logs data 221
   Windows Event Log 212

M
mail filter policy, blocking by
   file name 122
   individual file size 124
   mail subject 126
   message origin 128
   total file or message size 160
mail message update feature 122
multiple user accounts 73

N
nonviral threat
   categories of 117
notifications
   configuring 207
   logging 200

O
outbreak alerts 216

P
PFX certificate file 68
PKCS#12 certificate file 68
policy.xml 365
port number, configuring
   ICAP 98
POST transactions 97, 117
process priority 149
processing limits 161
product
   license 88, 93
protection, updating
   Rapid Release 243
   using Intelligent Update package 237
   using LiveUpdate 229
protocol
   ICAP 100
   RPC 100
   supported protocols 94
   supported services 95

Q
Quarantine 119
quarantine 114
queue size 81

R
Rapid Release
   about 243
   updating definitions
      automatically 244
      on demand 245
recursive scanning 350
resource 149
resource consumption 149, 152
   log file 152
return codes
   ICAP 393
   RPC 394
risks. See threats and security risks
RPC
   client IP address 103
   configuring 100
   notifying server of updated definitions 105
   notifying users of threat detection 138
   quarantining files 119
   return codes 394
   supported services 95
S

scan policy 261
scanning 347
See also command-line scanner
See also HTTP filtering
See also threats
improving performance 157, 160
scanning summary 222, 224
scanning thread 149
scans
licensing requirements 88, 93
specifying temporary scanning directory 81
security notice
about 80
enable or disable 80
self-test scanning 379
serial number 91
service startup properties
editing 108
silent installation
creating response file 326
generating encrypted password 336
initiating installation
Linux 331
Windows 335
installing
Linux 326
Windows 331
SMTP alerts
alert bind address 205
configuring 214
SNMP alerts
alert bind address 205
configuring 215
spyware
nonviral threat 117
SSL (Secure Socket Layer) 67
Symantec Insight™ 139
aggression level 142
Symantec Insight™ result parameters 140
Symantec Protection Engine
allocating resources 81
configuring using XML modifier command-line tool 365
installing 35
starting and stopping the daemon 61
starting and stopping the service 62
types of risks detected 110
Symantec Security Response 243
system requirements 30

T
telemetry 166
temporary scanning directory
specifying 81
third-party certificate 67
thread pool
maximum threads 81
XML modifier command-line tool 369
threat
advanced heuristic 118
detecting 117
detection 118
threats 110, 161
See also command-line scanner
See also container files
blocking by
file name 122
individual file size 124
mail subject 126
message origin 128
category 111
enabling detection 114
handling encrypted container files 134
handling malformed container files 132
handling partial container files 131
handling unscannable files 130
impact levels 111
quarantining files 119
testing detection capabilities 116

U
uninstallation 87
unscannable container file
partial container file 131
unscannable container files 130
encrypted container file 134
malformed container file 132
unscannable files 131–132, 134
upgrade 29
URL (Uniform Resource Locator) 167
URL categories
about 168
denying access 184
overriding URL categories 189
predefined categories 168
URL filtering
  about 168
  customizing the access denied message 190
  local categories 182
  See also
  modes 183
  URL categories 168
user accounts
  about 73
  Administrator 73
  create 74
  delete 78
  edit 76
  logs 73
  managing 73
  maximum number 73
  view 79
user notifications
  customizing 135, 190
  RPC-client users 138
UTF-8 encoding 126, 184, 365

V
view user accounts
  process 79
  visible details 79
virus 110, 161
  See also command-line scanner
  See also container files
blocking by
  file name 122
  individual file size 124
  mail subject 126
  message origin 128
enabling detection 114
handling encrypted container files 134
handling malformed container files 132
handling partial container files 131
handling unscannable files 130
quarantining files 119
testing detection capabilities 116

W
Windows
  installing Symantec Protection Engine 37
  uninstalling 87
  upgrading Symantec Protection Engine 43–44