Symantec™ Scan Engine Implementation Guide

Symantec™ Scan Engine Implementation Guide

Documentation version: 5.2.11

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Technical Support

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

Symantec's support offerings include the following:

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

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

www.symantec.com/business/support/

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

Contacting Technical Support

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

www.symantec.com/business/support/

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

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

- Product release level

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

Licensing and registration

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

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

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

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

Support agreement resources

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

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

Contents

Technical Support 4

Chapter 1 Introducing Symantec Scan Engine 13

About Symantec Scan Engine 13
What's new 14
Components of Symantec Scan Engine 15
How Symantec Scan Engine works 19
About Symantec Scan Engine deployment 20
About automatic load balancing 20
About supported protocols 21
What you can do with Symantec Scan Engine 23
Where to get more information 26

Chapter 2 Installing Symantec Scan Engine 27

Before you install 27
About running other antivirus products on the Symantec Scan Engine server 28
System requirements 28
Windows system requirements 29
Solaris system requirements 29
Linux system requirements 30
About installing Symantec Scan Engine 32
Installing Symantec Scan Engine on Windows 33
Installing Symantec Scan Engine on Linux 38
Installing Symantec Scan Engine on Solaris 42
Post-installation tasks 45
Verifying, stopping, and restarting the Symantec Scan Engine daemon on Linux and Solaris 46
Verifying, stopping, and restarting the Symantec Scan Engine service on Windows 47
Clearing the Java cache 48
Accessing the console 49
Enhancing security for the HTTPS servers and SSL servers 53
Changing the administrator settings 56
Allocating resources for Symantec Scan Engine 59

Migrating to version 5.2.11 64
About retaining the service account when you upgrade to version 5.2.11 65
About migrating from version 4.3x 65
Uninstalling Symantec Scan Engine 67

Chapter 3 Activating licenses 69

About licensing 69
About license activation 70
If you do not have a serial number 71
Obtaining a license file 71
Installing the license file 72
About removing license files 73
Checking the license status 73

Chapter 4 Configuring scanning services for client applications 75

About the communication protocols 75
Supported services by protocol 76
About working with ICAP 79
Configuring ICAP options 80
Working with the native protocol 82
Configuring native protocol options 83
Working with the RPC protocol 84
About RPC configuration options 85
Configuring Symantec Scan Engine to use the RPC protocol 86
Adding and removing RPC clients 87
Configuring RPC connection options 88
Configuring the RPC scanning policy 89
Notifying a file server when definitions are updated 90
Logging to the RPC client logging subsystem 91
User identification and notification when a risk is found 91
Editing the service startup properties 92

Chapter 5 Protecting against risks 95

About scanning for risks 95
How Symantec Scan Engine detects risks 96
Enabling threat detection 97
Ways to test threat detection capabilities 98
Quarantining infected files that cannot be repaired 99
Enabling security risk detection 100

About preventing potential threats 102
Configuring Symantec Scan Engine to block unscannable container files 103
Configuring file name filtering 105
Configuring file size filtering 107
Configuring subject line content filtering 108
Configuring message origin filtering 110
Customizing user notifications 111
Notifying RPC-client users that a threat was found 114

Chapter 6 Monitoring and tuning Symantec Scan Engine performance 115

How to monitor Symantec Scan Engine performance 115
Monitoring scanning requests 115
Monitoring Symantec Scan Engine resources 119
Ways to improve Symantec Scan Engine performance 121
Deployment considerations and recommendations 122
Enhance performance by limiting scanning 124
Configuration settings that can conserve and enhance performance 131

Chapter 7 Filtering URLs 133

About filtering URLs 133
About categories 134
How to filter a URL 148
About the filtering modes 148
Denying access to URLs in URL categories 150
Managing local categories 151
Overriding a URL categorization 154
Customizing the access denied message 155

Chapter 8 Logging data, issuing alerts, and generating reports 157

About logging data 157
Logging destinations 157
Logging levels and events 159
Specifying the log bind address 162
About configuring local logging 163
Specifying the local logging level 164
Changing the directory where log files are located 164
Maintaining log files on a shared resource 165

Changing the length of time that log files are maintained 166
Enabling statistics reporting 167
Configuring logging to the Windows Application Event Log 168
Configuring Symantec Scan Engine to log events to SSIM 169
About configuring alerts 170
Activating SMTP alerts 170
Activating SNMP alerts 171
Configuring outbreak alerts 173
About reports 174
Viewing the local log data 175
Exporting local log data to a file 176
Viewing statistics log data 176

Chapter 9 Keeping your product and protection up-to-date 179

About content updates 179
About definition updates 179
About updating your protection 180
About LiveUpdate 182
Configuring LiveUpdate to occur automatically 182
Performing LiveUpdate on demand 183
About scheduling LiveUpdate using the command-line 184
About setting up your own LiveUpdate server 184
About editing the LiveUpdate configuration file 184
About Intelligent Updater 187
Enabling definition updates through Intelligent Updater 188
About Rapid Release 190
Configuring Rapid Release updates to occur automatically 191
Performing Rapid Release updates on demand 192
Rolling back definitions 192

Appendix A Performing a silent installation 193

About silent installation and upgrade 193
Implementing a silent installation in Solaris and Linux 193
Creating the response file 194
About initiating a silent installation using the response file 197
About implementing a silent installation for Windows 197
Initiating a silent installation on Windows 199
Generating an encrypted password 200

Appendix B Using the Symantec Scan Engine command-line scanner 201

About the Symantec Scan Engine command-line scanner 201
Setting up a computer to submit files for scanning 202
C-based command-line scanner syntax and usage 203
Supported command-line options for C-based command-line scanner 204
About specifying the Symantec Scan Engine IP address and port for C-based command-line scanner 206
About specifying the antivirus scanning mode for C-based command-line scanner 207
About obtaining scan results for C-based command-line scanner 208
About requesting recursive scanning 211
About disposing of infected files when an error occurs 211
Excluding files from scanning 211
Redirecting console output to a log file 212
Java-based command-line scanner syntax and usage 213
Supported command-line options for Java-based command-line scanner 213
About specifying the Symantec Scan Engine IP address and port for java-based command-line scanner 215
About specifying the antivirus scanning mode for Java-based command-line scanner 216
About obtaining scan results for Java-based command-line scanner 216

Appendix C Editing configuration data 219

Editing the Symantec Scan Engine configuration files 219
How to use the XML modifier command-line tool 220
Accessing the XML modifier command-line tool 220
About option commands 221
About configuration options 222
Configuring the ICAP response 224
Configuring the ICAP preview option 224
Controlling the dynamic thread pool 225
Disabling the ICAP threshold client notification 227
Specifying maximum lengths for file names 228
Specifying whether to scan top-level files 228
Configuring the number of LiveUpdate retries 229
Changing the LiveUpdate base time 229

Extracting all streams from OLE-structured storage documents for scanning 229
Specifying a replacement file name 230
Specifying archive file types to scan 230
Modifying the ICAP options attribute-list extension 231
Modifying the ICAP response to send the non-viral threat category name 232
Accessing scan error files 232
Deleting or repairing infected read-only files 232
Disabling automatic self-test scanning 233
Enabling non-viral threat categories information 234
Specifying decomposer file size limit 235
Specifying maximum file size for extracted files 235
Specifying maximum cumulative file size for extracted files 236
Specifying the maximum socket time-out value 236

Appendix D Return codes 239

Native protocol return codes 239
ICAP return codes 240
RPC protocol return codes 241

Glossary 243

Index 247

Chapter 1

Introducing Symantec Scan Engine

This chapter includes the following topics:

- About Symantec Scan Engine
- What's new
- Components of Symantec Scan Engine
- How Symantec Scan Engine works
- What you can do with Symantec Scan Engine
- Where to get more information

About Symantec Scan Engine

Symantec™ Scan Engine is a carrier-class content scanning engine. Symantec Scan Engine provides content scanning capabilities to any application on an IP network, regardless of platform. Any application can pass files to Symantec Scan Engine for scanning.

Symantec Scan Engine accepts scan requests from client applications that use any of the following protocols:

- Symantec Scan Engine native protocol
- The *Internet Content Adaptation Protocol* (ICAP), version 1.0, as presented in RFC 3507 (April 2003)
- A proprietary implementation of remote procedure call (RPC)

See "About supported protocols" on page 21.

Use the Symantec Scan Engine software development kit (SDK) to integrate Symantec Scan Engine with your application. The SDK supports version 1.0 of ICAP, as presented in RFC3507 (April 2003). Symantec also has developed connector code for some third-party applications to seamlessly integrate with Symantec Scan Engine.

What's new

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

Table 1-1 New features

Feature	Description
Enhanced URL Filtering	Symantec Scan Engine is integrated with an enhanced URL database. The URL database now contains Symantec URL categories and Child Abuse Image Content (CAIC) URL categories to scan and block the unwanted URLs. See "About filtering URLs" on page 133.
Maximum extract size limit for container files increased upto 30GB	Symantec Scan Engine can now process specific container types of size up to 30 GB. A new parameter called `DecFileSize` allows Symantec Scan Engine to decompose top-level container files of type tar/rar/zip up to 30 GB. For other container types, the maximum top-level container file size can be up to 2 GB. See "Specifying decomposer file size limit" on page 235. For individual files within tar/rar/zip containers, you can specify the existing `MaxExtractSize` parameter to have a value up to 30719 MB (~30 GB). For other container types, the maximum extract file size that you can specify for individual files can be up to 1907 MB (~2 GB). See "Specifying maximum file size for extracted files" on page 235. See "Setting container file limits" on page 129. Symantec Scan Engine calculates the cumulative file size after each file is extracted. The `MaxCumulativeExtractSize` parameter stops the recursive scanning of individual files once this file size limit is reached. This parameter accepts a maximum value of 32212254720 bytes (~30 GB). See "Specifying maximum cumulative file size for extracted files" on page 236.

Table 1-1 New features *(continued)*

Feature	Description
Extended support for C API to 64-bit platforms	From Symantec Scan Engine 5.2.11 onwards, the C API contains libraries for the following 64-bit platforms: ■ Windows Server 2008 R2 -64 bit (using Microsoft Visual Studio 2008 version 9.0) ■ RHEL 5.5 -64 bit (using gcc 4.1.2) ■ Solaris 10 (SPARC) -64 bit (using gcc 3.4.3) ■ Solaris 10 (x86) -64 bit (using gcc 3.4.3) For more information, see the *Symantec Scan Engine Software Developer's Guide*.
Additional platform support for C API	You can now compile the C API libraries on the following new platforms: ■ Sun Solaris 10 (x86) - 32 bit (using gcc 3.4.3) ■ Sun Solaris 10 (x86) - 64 bit (using gcc 3.4.3) For more information, see the *Symantec Scan Engine Software Developer's Guide*.
Support for AMD Opteron ™ Processors	From Symantec Scan Engine 5.2.11 onwards, Symantec Scan Engine supports AMD Opteron ™ (1.4 GHz or higher) processors.
Default Server Resources values increased	The default value for the maximum RAM used for in-memory file system has now increased from 16 MB to 128 MB. The default value for the maximum file size stored within the in-memory file system has now increased from 3 MB to 16 MB.

Components of Symantec Scan Engine

Table 1-2 lists the components that are included on the product CD.

Table 1-2 Product components

Component	Description	Folder name
Symantec Scan Engine	The software that you install to protect your network from threats (such as viruses), security risks (such as adware and spyware), and unwanted content.	Scan_Engine\

Table 1-2 Product components *(continued)*

Component	Description	Folder name
Silent installation	The files that you can use to perform a silent installation or upgrade. Also includes response files for Red Hat and Solaris.	Scan_Engine\Silent_Install\
Command-line scanner	The software that acts as a client to Symantec Scan Engine through the Symantec Scan Engine application programming interface (API). The command-line scanner lets you send files to Symantec Scan Engine to be scanned.	Command-Line_Scanner\
Symantec Scan Engine software developer's kit	The tools and information that you can use to create the customized integrations that use ICAP.	Scan_Engine_SDK\
Symantec Central Quarantine server	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.	Tools\Central_Quarantine\

Table 1-2 Product components *(continued)*

Component	Description	Folder name
LiveUpdate™ Administration Utility	The utility that you use to configure one or more intranet FTP, 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. For more information, see the *LiveUpdate Administrator's Guide* on the product CD.	Tools\LiveUpdate_Admin\

Table 1-2 Product components *(continued)*

Component	Description	Folder name
Microsoft Operations Manager 2005 (MOM) Pack	You can integrate Symantec Scan Engine events with Microsoft Operations Manager 2005. Microsoft Operations Manager is a central repository that can receive critical events, errors, warnings, and other information from your Symantec Scan Engine servers. Preconfigured Rule Groups and Child Rule Groups are automatically created when you import the management pack. These rules monitor specific Symantec Scan Engine events in the Windows Event Log. When a rule is triggered, the Microsoft Operations Manager agent collects data about the event and forwards it to the Microsoft Operations Manager. For more information, see the *Symantec™ Scan Engine Management Pack Integration Guide* on the Symantec Scan Engine product CD.	Tools/MOM_Management_Pack/
Java™ 2SE Runtime Environment (JRE) 5.0 and 6.0	The software that is required to access the Symantec Scan Engine console.	Tools\Java\

Table 1-2 Product components *(continued)*

Component	Description	Folder name
Symantec pcAnywhere (host only version)	A software solution that lets Symantec Technical Support access your computer remotely. This restricted version of pcAnywhere should only be installed when requested by Symantec support. Symantec pcAnywhere host version is for Windows platforms only.	Technical_Support\Win32

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/.

How Symantec Scan Engine works

Symantec Scan Engine supports several options for creating custom integrations between Symantec Scan Engine and any C, C++, Java, and .Net application that supports ICAP.

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

- Client-side antivirus application program interface (API) C library
  If you plan to integrate content scanning, you can use the antivirus API. HTTP content filtering and security risk scanning are not available with the antivirus API.
- Standard ICAP, based on the specification that is presented in RFC 3507 (April 2003)

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

You can configure client applications to pass files to Symantec Scan Engine through one of the supported communication protocols. You can configure Symantec Scan 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.

The *Symantec Scan Engine Software Developers Guide* provides information about how to create customized integrations with ICAP. Symantec also provides a number of connectors for Symantec Scan Engine to make the integration with some third-party applications easier. Other software companies have developed

connectors for Symantec Scan Engine to provide content scanning for their products.

If you have purchased Symantec Scan Engine with a connector, you might need to configure Symantec Scan Engine to work with the connector. You might also need to configure the third-party application to add threat, security risk, and URL scanning. Consult any documentation that is included with the connector in addition to this guide.

About Symantec Scan Engine deployment

A client application is an application that is configured to pass files to Symantec Scan Engine for scanning. In a typical configuration, Symantec Scan Engine runs on a separate computer. The client application passes files to Symantec Scan Engine through a socket over the network. Based on the network setup, client applications can pass a full path rather than the actual file to Symantec Scan Engine. For example, files to be scanned might be located on a drive that can be mounted over the network. If the client application and Symantec Scan Engine have access to a shared directory, the client application can place the file in the shared directory. The client application can then pass the full path to Symantec Scan Engine. This shared directory lets Symantec Scan Engine access the file directly.

When the client application runs on the same computer as Symantec Scan Engine and Symantec Scan Engine has access to the file, the client application only passes the file name. Symantec Scan Engine opens the file and scans it in place on the computer. In some instances, the client receives the file in chunks, and it forwards the chunks to Symantec Scan Engine. In this case, Symantec Scan Engine does stream-based scanning rather than in-place scanning.

About automatic load balancing

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

If any Symantec Scan Engine cannot be reached or fails during a scan, another Symantec Scan Engine is called. The faulty Symantec Scan Engine is taken out of rotation for a period of time. If all of the Symantec Scan Engines are out of rotation, the faulty Symantec Scan Engines are called again.

If your client uses ICAP, the ICAP threshold client notification feature is enabled by default. When the number of queued requests for a Symantec Scan Engine

exceeds its threshold, Symantec Scan 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 Scan Engine benefit from load-balanced scanning without any additional effort.

See "Allocating resources for Symantec Scan Engine" on page 59.

See "Disabling the ICAP threshold client notification" on page 227.

The API keeps trying to contact Symantec Scan Engine unless one of the following events occur:

- Five or more engines are not functioning
- It appears that a file that was scanned might have caused more than one Symantec Scan Engine to fail

If you use Symantec Scan Engine as a plug-in with RPC or ICAP, you might be able to configure the load balancing across multiple Symantec Scan Engines. This reconfiguration depends on the implementation. For more information, see the documentation for the plug-in.

About supported protocols

Table 1-3 lists the supported protocols that client applications can use to send scan requests to Symantec Scan Engine.

Table 1-3 Supported protocols

Protocol	Description
Native protocol	Symantec Scan Engine implements a TCP/IP protocol to provide scanning functionality to client applications. This protocol is text-based, like HTTP or SMTP. It uses ASCII commands and responses to communicate between the client and the server. To scan a file, a client connects to the default IP port. It sends the file to be scanned and then reads the results of the scan. After the client receives the scan results, the client and server disconnect and must initiate a new connection to scan each subsequent file. See "Working with the native protocol" on page 82.

Table 1-3 Supported protocols *(continued)*

Protocol	Description
Internet Content Adaptation Protocol (ICAP)	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 Scan Engine. It can also request the scanning of the content that is retrieved from the Web. See "About working with ICAP" on page 79.
A proprietary remote procedure call (RPC) protocol	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 Scan Engine uses a proprietary scanning protocol with the MS-RPC protocol to interface with client applications. This protocol is supported only on Windows 2000 Server/Windows 2003 Server/Windows 2008 Server. Any appropriate client can use RPC to communicate with Symantec Scan Engine to request the scanning and repairing of files. See "Working with the RPC protocol" on page 84.

See "Supported services by protocol" on page 76.

What you can do with Symantec Scan Engine

Table 1-4 lists the tasks that you can perform with Symantec Scan Engine.

Table 1-4 What you can do with Symantec Scan Engine

Task	Description
Configure protocols to pass files to Symantec Scan Engine for scanning	You can change the communication protocol that Symantec Scan Engine uses to communicate with the client applications for which it provides scanning services. The features that are available through Symantec Scan Engine differ depending on the protocol that you use. You can use any of the following protocols: ■ Native protocol ■ ICAP ■ RPC After you select a protocol, you must provide protocol-specific configuration information. The configuration options differ depending on the protocol that you select. See "About the communication protocols" on page 75.
Detect threats	You can configure Symantec Scan Engine to scan files and email messages for threats, such as viruses and Trojan horses. You can establish policies to process the documents that contain threats. You can also quarantine the infected files that cannot be repaired. See "Enabling threat detection" on page 97. See "Quarantining infected files that cannot be repaired" on page 99.
Prevent potential threats	You can filter files and email messages to further protect your network. See "Configuring file size filtering" on page 107. See "Configuring file name filtering" on page 105. See "Configuring subject line content filtering" on page 108. See "Configuring message origin filtering" on page 110. Symantec Scan Engine can also block certain types of the container files that might contain threats or malicious code. See "Configuring Symantec Scan Engine to block unscannable container files" on page 103.

Table 1-4 What you can do with Symantec Scan Engine *(continued)*

Task	Description
Detect security risks	Symantec Scan Engine can detect security risks such as: adware, dialers, hacking tools , joke programs, remote access programs, spyware, and trackware. See "Enabling security risk detection" on page 100.
Prevent denial-of-service attacks	Symantec Scan Engine protects your network from the file attachments that can overload the system and cause denial-of-service attacks. Denial-of-service attacks can include any of the following types of container files: ■ Files that are overly large ■ Files that contain large numbers of embedded, compressed files ■ Files that are designed to maliciously use resources and degrade performance. To reduce your exposure to denial-of-service threats, you can impose limits to control how Symantec Scan Engine handles container files. See "Setting container file limits" on page 129.
Specify the files to scan	You can conserve bandwidth and time if you limit the files and messages that are scanned. See "Specifying which files to scan" on page 125. See "Specifying the maximum file or message size to scan" on page 128.
Filter HTTP requests for unwanted content	If your client uses ICAP, you can apply Uniform Resource Locator (URL) filtering to block access to sites that contain unwanted content. Symantec Scan Engine uses Symantec URL categories and Child Abuse Image Content (CAIC) URL categories to scan and block the unwanted URLs. See "About categories" on page 134.

Table 1-4 What you can do with Symantec Scan Engine *(continued)*

Task	Description
Customize user notifications	Symantec Scan Engine lets you customize messages to users to notify them when a file has been infected, repaired, 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. See "Customizing user notifications" on page 111. See "Customizing the access denied message" on page 155.
Log events and review event data and statistics	Symantec Scan 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 Scan Engine generates log messages. Use the Symantec Scan Engine reporting functionality to view your log data and statistics. See "About logging data" on page 157.
Issue alerts	Symantec Scan Engine can send alerts through Simple Mail Transfer Protocol (SMTP) and Simple Network Management Protocol (SNMP). You also can activate outbreak alerts. Symantec Scan 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 170.
Monitor Symantec Scan Engine performance	You can monitor Symantec Scan 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 Scan Engine performance" on page 115.
Keep your protection up-to-date	You can update your content for Symantec Scan Engine. Content updates ensure that your network is up-to-date with the most current risk and URL definitions. You also can update Symantec Scan Engine with the latest definitions without any interruption to scanning or filtering operations. See "About content updates" on page 179.

Table 1-4 What you can do with Symantec Scan Engine *(continued)*

Task	Description
Perform tasks from the command-line scanner	The command-line scanner acts as a client to Symantec Scan Engine through the Symantec Scan Engine API. Use the command-line scanner to send files to Symantec Scan 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 scan engine operation. See "About the Symantec Scan Engine command-line scanner" on page 201.

Where to get more information

Symantec Scan 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 Scan Engine console.

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

The following online resources are available:

Provides access to the technical support Knowledge Base, newsgroups, contact information, downloads, and mailing list subscriptions	www.symantec.com/techsupp/ent/enterprise.html
Provides information about registration, frequently asked questions, how to respond to error messages, and how to contact Symantec License Administration	www.symantec.com/licensing/els/help/en/help.html
Provides product news and updates	www.enterprisesecurity.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	www.symantec.com/security_response/index.jsp

Chapter 2

Installing Symantec Scan Engine

This chapter includes the following topics:

- Before you install
- System requirements
- About installing Symantec Scan Engine
- Post-installation tasks
- Migrating to version 5.2.11
- Uninstalling Symantec Scan Engine

Before you install

Install Symantec Scan Engine on a computer that meets the system requirements. Before you install Symantec Scan 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 28.

Before you install Symantec Scan engine, take the following steps:

- Install Java 2SE Runtime Environment (JRE) 5.0 (update 13 or later) or JRE 6.0 on the server.
  The most current version of JRE 5.0 and JRE 6.0 at the time of product ship is provided on the product CD in the following folder:
  \Tools\Java*operating system platform*

- Disable any third-party antivirus products that are running on the server on which you plan to install Symantec Scan Engine.
  After installation is complete, you can re-enable antivirus protection.

  Note: Run another Symantec antivirus product on the server that runs Symantec Scan Engine to protect the server from threats.

  See "About running other antivirus products on the Symantec Scan Engine server" on page 28.

- Review the deployment considerations and recommendations. These recommendations could enhance your overall performance.
  See "Deployment considerations and recommendations" on page 122.

After you complete the installation, perform the post-installation tasks.

See "Post-installation tasks" on page 45.

About running other antivirus products on the Symantec Scan Engine server

Symantec Scan Engine scans the files that client applications pass to Symantec Scan Engine. Symantec Scan Engine does not protect the computer on which it runs. Since Symantec Scan Engine processes 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 Scan Engine runs, such as Symantec AntiVirus Corporate Edition. To prevent scanning conflicts, configure the antivirus program not to scan the temporary directory that Symantec Scan Engine uses for scanning.

See "Allocating resources for Symantec Scan Engine" on page 59.

System requirements

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

See "Windows system requirements" on page 29.

See "Solaris system requirements" on page 29.

See "Linux system requirements" on page 30.

Windows system requirements

The following are the system requirements for Windows.

Operating system	■ Windows 2000 Server with the latest service pack ■ Windows Server 2003 (32-bit) ■ Windows Server 2003 Japanese (32-bit) ■ Windows Server 2003 R2 (32-bit and 64-bit) ■ Windows Server 2008 (32-bit and 64-bit) ■ Windows Server 2008 R2 (64-bit)
Processor	Pentium 4 processor 3.4 GHz or higher
Memory	2 GB of RAM or higher
Disk space	2 GB of hard disk space 10 GB of hard disk space for using URL Filtering feature
Hardware	■ 1 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	■ J2SE Runtime Environment (JRE) 5.0 (update 13 or later) or JRE 6.0 The most current version of JRE 5.0 and JRE 6.0 at the time of product ship is provided on the product CD in the following folder: \Tools\Java\Win32 ■ One of the following Web browsers to access the Symantec Scan Engine console ■ Microsoft Internet Explorer 6 (SP1) or later Use Microsoft Internet Explorer to access the Symantec Scan Engine console from a Windows client computer. ■ Mozilla Firefox 1.5 or later Use Mozilla Firefox to access the Symantec Scan Engine console from a Solaris or Linux client computer. The Web browser is only required for Web-based administration. You must install the Web browser on a computer from which you want to access the Symantec Scan Engine console. The computer must have access to the server on which Symantec Scan Engine runs.

Solaris system requirements

The following are the system requirements for Solaris:

Operating system	Solaris 9 and 10 Ensure that your operating system has the latest service patches that are available.
Processor	SPARC® 3.4 GHz or higher
Memory	2 GB of RAM or higher
Disk space	2 GB of hard disk space 10 GB of hard disk space for using URL Filtering feature
Hardware	■ 1 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	■ J2SE Runtime Environment (JRE) 5.0 (update 13 or later) or JRE 6.0 The most current version of JRE 5.0 and JRE 6.0 at the time of product ship is provided on the product CD in the following folder: \Tools\Java\Solaris If you install the self-extracting JRE, 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 Scan Engine console: ■ Mozilla Firefox 1.5 or later Use Mozilla Firefox to access the Symantec Scan Engine console from a Solaris or Linux client computer. ■ Microsoft Internet Explorer 6 (SP1) or later Use Microsoft Internet Explorer to access the Symantec Scan Engine console from a Windows client computer. The Web browser is only required for Web-based administration. You must install the Web browser on a computer from which you want to access the Symantec Scan Engine console. The computer must have access to the server on which Symantec Scan Engine runs.

Linux system requirements

The following are the system requirements for Linux:

Operating system	■ Red Hat Linux Enterprise Server 3 and 4 ■ Red Hat Linux Advanced Server 3 and 4 ■ Red Hat Enterprise Linux 5 (32-bit and 64-bit) ■ SUSE Linux Enterprise Server 9 (32-bit) ■ SUSE Linux Enterprise Server 10 and 11 (32-bit and 64-bit)
Processor	Pentium 4 processor 3.4 GHz or higher
Memory	2 GB of RAM or higher
Disk space	2 GB of hard disk space 10 GB of hard disk space for using URL Filtering feature
Hardware	■ 1 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: ■ GNU sharutils-4.6.1-2 or later Use this package to expand the Rapid Release packages. ■ ncompress-4.2.4-44 or later Use this package to expand the Rapid Release packages. ■ GNU C Library (glibc) ■ initscripts This package is required for Red Hat Linux only. ■ aaa_base package This package is required for SUSE only. ■ J2SE Runtime Environment (JRE) 5.0 (update 13 or later) or JRE 6.0 The most current version of JRE 5.0 and JRE 6.0 at the time of product ship is provided on the product CD in the following folder: \Tools\Java\RedHat Install the 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 Scan Engine console: ■ Mozilla Firefox 1.5 or later Use Mozilla Firefox to access the Symantec Scan Engine console from a Solaris or Linux client computer. ■ Microsoft Internet Explorer 6 (SP1) or later Use Microsoft Internet Explorer to access the Symantec Scan Engine console from a Windows client computer. The Web browser is only required for Web-based administration. You must install the Web browser on a computer from which you want to access the Symantec Scan Engine console. The computer must have access to the server on which Symantec Scan Engine runs.

About installing Symantec Scan Engine

The Symantec Scan Engine installation program checks for previous versions of the product. The results of the check determine what happens next:

No previous version is detected.	A full installation is performed.

Version 5.2, 5.1, or 4.3x is detected.	Symantec Scan Engine supports upgrades from version 5.2, 5.1, and 4.3x. You can select whether to upgrade the product and preserve your existing settings or to perform a clean installation. If you choose to do a clean installation, the installer removes the previous installation, and then installs the new version as a full installation. See "Migrating to version 5.2.11" on page 64.
Version 5.0	Symantec Scan Engine does not support upgrades from version 5.0. If you are using version 5.0, uninstall version 5.0 and then install version 5.2.11.

Note: Symantec Scan Engine cannot be installed in high-ASCII and DBCS directories.

During installation, Symantec Scan Engine installs a virtual administrative account. You are recommended to remember the password for this account as it is the only account used to manage Symantec Scan Engine. If you want to change the password in the console, you must have the old password.

See "Accessing the console" on page 49.

After you install Symantec Scan Engine, activate all applicable licenses. If you upgrade from a previous version that has valid licenses, when the installation is complete, Symantec Scan Engine automatically recognizes these licenses.

See "About licensing" on page 69.

Symantec Scan 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 scanning.

See "About filtering URLs" on page 133.

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

If you need to install or upgrade multiple Symantec Scan 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 193.

Installing Symantec Scan Engine on Windows

You can install Symantec Scan Engine on Windows servers. If you cancel the installation process during an upgrade, you might need to restart the service.

(The service is stopped when the installer detects an upgrade.) When the installation is complete, Symantec Scan Engine is installed as a Windows 2000/2003/2008 service. It is listed as Symantec Scan Engine in the Services Console. The Symantec Scan Engine service starts automatically when the installation is complete. Any significant installation activities are recorded in the Windows Application Event Log.

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

See "System requirements" on page 28.

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 Scan Engine on Windows" on page 34.
- Upgrade from a previous version and retain existing settings
  See "To upgrade Symantec Scan Engine on Windows" on page 35.
- Perform a clean upgrade
  Uninstalls your current version of Symantec Scan Engine and installs version 5.2.11
  See "To upgrade Symantec Scan Engine on Windows" on page 35.
  See "To configure clean upgrade installation options on Windows" on page 37.

To install Symantec Scan Engine on Windows

1. Log on to the computer on which you plan to install Symantec Scan Engine as administrator or as a user with administrator rights.
2. On the Symantec Scan Engine installation CD, run ScanEngine.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 Scan Engine, and then click **Next**.

   The default location is C:\Program Files\Symantec\Scan Engine for 32-bit Windows platform, and C:\Program Files (x86)\Symantec\Scan Engine for 64-bit Windows platform.

6 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 Scan Engine by editing the configuration file. See "Editing the Symantec Scan Engine configuration files" on page 219.
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 a SSL port that is not in use by any other program or service. Use a port number that is greater than 1024.
Administrator Password	Type a password for the virtual administrative account that you intend to use to manage Symantec Scan Engine.
Confirm Administrator Password	Confirm the password by typing it again.

7 Click **Next**.

8 In the URL filtering panel, select the provided option to enable URL filtering feature and downloading of URL definitions.

You can also change the setting after installation. Go to Policies > Filtering > URL to enable this option.

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

10 Click **Finish**.

To upgrade Symantec Scan Engine on Windows

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

2 On the Symantec Scan Engine installation CD, run ScanEngine.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 Scan Engine panel, select one of the following upgrade options:

Preserve existing settings (upgrades your version of Symantec Scan Engine while preserving your existing settings)	Do all of the following steps: ■ Click **Upgrade and preserve existing settings, configuration and data**. ■ If the previous version runs under an account other than the Local System account, Symantec Scan Engine automatically populates the service account name (non-editable) in the **Symantec Scan Engine Credentials** screen. Type the password for this service account. The **Symantec Scan Engine Service Credentials** screen appears only if the previous version of Symantec Scan Engine runs on an account other than Local System. ■ Click **Next**. ■ If the password is incorrect,an invalid credentials screen appears. Click **Back** to try the service account password again. Alternatively, click **Next** to continue the upgrade without a service account password. However, the Symantec Scan Engine service does not start after installation. Once the installation is complete, you must type the correct service account password and start the service manually. ■ Click **Install**. ■ When the installer is complete, click **Finish**. See "Verifying, stopping, and restarting the Symantec Scan Engine service on Windows" on page 47.
Clean upgrade (uninstalls your version of Symantec Scan Engine and installs version 5.2.11)	Do all of the following steps: ■ Click **Clean upgrade. Do not preserve any existing settings, configuration or data**. ■ Click **Next**. ■ Configure the clean upgrade configuration options. See "To configure clean upgrade installation options on Windows" on page 37.

To configure clean upgrade installation options on Windows

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

The default location is C:\Program Files\Symantec\Scan Engine for 32-bit Windows platform, and C:\Program Files (x86)\Symantec\Scan Engine for 64-bit Windows platform.

2 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 Scan Engine by editing the configuration file. See "Editing the Symantec Scan Engine configuration files" on page 219.
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 a SSL port that is not in use by any other program or service. Use a port number that is greater than 1024.
Administrator Password	Type a password for the virtual administrative account that you intend to use to manage Symantec Scan Engine.
Confirm Administrator Password	Confirm the password by typing it again

3 Click **Next**.

4 In the URL filtering panel, select the provided option to enable URL filtering feature and downloading of URL definitions.

You can also change the setting after installation. Go to Policies > Filtering > URL to enable this option.

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

6 Click **Finish**.

Installing Symantec Scan Engine on Linux

You can install Symantec Scan 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 initiate the installer for Linux" on page 38.
  See "To install Symantec Scan Engine on Linux" on page 39.
- Upgrade from a previous version and retain existing settings
  See "To initiate the installer for Linux" on page 38.
  See "To upgrade Symantec Scan Engine on Linux" on page 40.
- Perform a clean upgrade
  Uninstalls your current version of Symantec Scan Engine and installs version 5.2.11
  See "To initiate the installer for Linux" on page 38.
  See "To upgrade Symantec Scan Engine on Linux" on page 40.
  See "To configure clean upgrade installation options on Linux" on page 41.

To initiate the installer for Linux

1. Login to the computer on which you want to install Symantec Scan Engine as root.
2. Change directories to the location where the ScanEngine.sh file is located on the product CD.

   <drive>:\Scan_Engine\RedHat\
3. Type the following command:

   ```
   ./ScanEngine.sh
   ```

To install Symantec Scan Engine on Linux

1. Indicate the location where JRE 5.0 (update 13 or later) or JRE 6.0 is located.

   You only need to provide this information if the installer does not find the appropriate version. If you need to install the most current version of JRE 5.0 or JRE 6.0, it is included on the product CD in the following location:

   \Tools\Java\RedHat

   JRE 5.0 (update 13 or later) or JRE 6.0 must be installed to continue the product installation.

2. After you review with the Symantec license agreement, press **Y** to indicate that you agree with the terms of the agreement.

   If you indicate No, the installation is canceled.

3. Select the location to install Symantec Scan Engine, and then press **Enter**.

   The default location is /opt/SYMCScan.

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

Yes	Symantec Scan Engine is installed to run as root.
No	Symantec Scan Engine is installed not to run as root. Default setting.

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

   The user account must already exist.

6. 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 Scan Engine by editing the configuration data XML file.

   See "Editing the Symantec Scan Engine configuration files" on page 219.

7. 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 a SSL port that is not in use by any other program or service. Use a port number that is greater than 1024.

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

9 Press **Y** to specify if you want to enable URL filtering and download URL definitions.

You can also change the setting after installation. Go to Policies > Filtering > URL to enable this option.

The installer proceeds from this point with the installation.

See "Post-installation tasks" on page 45.

To upgrade Symantec Scan Engine on Linux

1 Indicate the location where JRE 5.0 (update 13 or later) or JRE 6.0 is located.

You only need to provide this information if the installer does not find the appropriate version. If you need to install the most current version of JRE 5.0 or JRE 6.0, it is included on the product CD in the following location:

\Tools\Java\RedHat

JRE 5.0 (update 13 or later) or JRE 6.0 must be installed to continue the product installation.

2 After you review with the Symantec license agreement, press **Y** to indicate that you agree with the terms of the agreement.

If you indicate No, the installation is canceled.

3 Select the type of upgrade that you want to perform as follows:

1	Clean upgrade Existing settings are not preserved. See "To configure clean upgrade installation options on Linux" on page 41.
2	Preserve existing settings Existing settings are preserved. If you choose to preserve your existing settings, the installer proceeds from this point with the installation. No further actions are required. See "Post-installation tasks" on page 45.

To configure clean upgrade installation options on Linux

1. Select the location to install Symantec Scan Engine, and then press **Enter**.

   The default location is /opt/SYMCScan.

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

Yes	Symantec Scan Engine is installed to run as root.
No	Symantec Scan Engine is installed not to run as root. Default setting.

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

   The user account must already exist.

4. 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 Scan Engine by editing the configuration data XML file.

   See "Editing the Symantec Scan Engine configuration files" on page 219.

5. 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 a SSL port that is not in use by any other program or service. Use a port number that is greater than 1024.

6. Type a password for the virtual administrator, and then confirm the password by typing it again.

7. Press **Y** to specify if you want to enable URL filtering and download URL definitions.

   You can also change the setting after installation. Go to Policies > Filtering > URL to enable this option.

   The installer proceeds from this point with the installation.

   See "Post-installation tasks" on page 45.

Installing Symantec Scan Engine on Solaris

You can install Symantec Scan 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 initiate the installer for Solaris" on page 42.
  See "To install Symantec Scan Engine on Solaris" on page 43.
- Upgrade from a previous version and retain existing settings
  See "To initiate the installer for Solaris" on page 42.
  See "To upgrade Symantec Scan Engine on Solaris" on page 44.
- Perform a clean upgrade
  Uninstalls your current version of Symantec Scan Engine and installs version 5.2.11
  See "To initiate the installer for Solaris" on page 42.
  See "To upgrade Symantec Scan Engine on Solaris" on page 44.
  See "To configure clean upgrade installation options on Solaris" on page 44.

To initiate the installer for Solaris

1. Login to the computer on which you want to install Symantec Scan Engine as root.
2. Change directories to the location where the ScanEngine.sh file is located on the product CD.

   <drive>:\Scan_Engine\Solaris\
3. Type the following command:

   ```
   ./ScanEngine.sh
   ```

To install Symantec Scan Engine on Solaris

1. Indicate the location where JRE 5.0 (update 13 or later) or JRE 6.0 is located.

   You only need to provide this information if the installer does not find the appropriate version. If you need to install the most current version of JRE 5.0 or JRE 6.0, it is included on the product CD in the following location:

   \Tools\Java\Solaris

   JRE 5.0 (update 13 or later) or JRE 6.0 must be installed to continue the product installation.

2. After you review with the Symantec license agreement, press **Y** to indicate that you agree with the terms of the agreement.

   If you indicate No, the installation is canceled.

3. Select the location to install Symantec Scan Engine, and then press **Enter**.

   The default location is /opt/SYMCScan.

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

Yes	Symantec Scan Engine is installed to run as root.
No	Symantec Scan Engine is installed not to run as root. Default setting.

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

   The user account must already exist.

6. 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 Scan Engine by editing the configuration data XML file.

   See "Editing the Symantec Scan Engine configuration files" on page 219.

7. 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 a SSL port that is not in use by any other program or service. Use a port number that is greater than 1024.

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

9 Press Y to specify if you want to enable URL filtering and download URL definitions.

You can also change the setting after installation. Go to Policies > Filtering > URL to enable this option.

The installer proceeds from this point with the installation.

See "Post-installation tasks" on page 45.

To upgrade Symantec Scan Engine on Solaris

1 Indicate the location where JRE 5.0 (update 13 or later) or JRE 6.0 is located.

You only need to provide this information if the installer does not find the appropriate version. If you need to install the most current version of JRE 5.0 or JRE 6.0, it is included on the product CD in the following location:

\Tools\Java\Solaris

JRE 5.0 (update 13 or later) or JRE 6.0 must be installed to continue the product installation.

2 Select the type of upgrade that you want to perform as follows:

1	Clean upgrade Existing settings are not preserved. See "To configure clean upgrade installation options on Solaris" on page 44.
2	Preserve existing settings Existing settings are preserved. If you choose to preserve your existing settings, the installer proceeds from this point with the installation. No further actions are required. See "Post-installation tasks" on page 45.

To configure clean upgrade installation options on Solaris

1 Press **Y** to confirm your understanding that Symantec Scan Engine cannot be installed if you quit at any time during the installation process.

2 After you review with the Symantec license agreement, press **Y** to indicate that you agree with the terms of the agreement.

If you indicate No, the installation is canceled.

3 Select the location to install Symantec Scan Engine, and then press **Enter**.

The default location is /opt/SYMCScan.

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

Yes	Symantec Scan Engine is installed to run as root.
No	Symantec Scan Engine is installed not to run as root. Default setting.

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

The user account must already exist.

6 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 Scan Engine by editing the configuration data XML file.

See "Editing the Symantec Scan Engine configuration files" on page 219.

7 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 a SSL port that is not in use by any other program or service. Use a port number that is greater than 1024.

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

9 Press Y to specify if you want to enable URL filtering and download URL definitions.

You can also change the setting after installation. Go to Policies > Filtering > URL to enable this option.

The installer proceeds from this point with the installation.

See "Post-installation tasks" on page 45.

Post-installation tasks

The post-installation tasks are as follows:

- Verifying, stopping, and restarting the Symantec Scan Engine daemon on Linux and Solaris
- Verifying, stopping, and restarting the Symantec Scan Engine service on Windows
- Clearing the Java cache
- Accessing the console
- Enhancing security for the HTTPS servers and SSL servers
- Allocating resources for Symantec Scan Engine

Verifying, stopping, and restarting the Symantec Scan Engine daemon on Linux and Solaris

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

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

To verify that the Symantec Scan Engine daemon is running on Linux and Solaris

1 At the command prompt, type the following command:

```
ps -ea | grep sym
```

A list of processes similar to the following appears:

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

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

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

```
/etc/init.d/symcscan restart
```

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

To stop and restart the Symantec Scan Engine daemon on Solaris and Linux

1 Login 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`

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

Symantec Scan 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 version 5.2.11. You can type the service account password when you upgrade. However, if the password is incorrect, you can continue the upgrade but Symantec

Scan 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 Scan Engine service. When you do, the client applications that are submitting files for scanning can lose their connection to Symantec Scan Engine. The client applications must reestablish their connections and resubmit files for scanning.

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

To verify that the Symantec Scan 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 Scan Engine**.
4. Verify that the status indicates Started.

To stop and restart the Symantec Scan 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 Scan 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**.

Clearing the Java cache

In some configurations, the caching of Java applets might cause the Symantec Scan Engine console to display very slowly or fail to display at all. To prevent this problem, 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. Click **View Applets**.

3 Select all of the items in the table and click **Delete**.

4 Uncheck **Enable Caching**.

This step disables the Java caching feature.

5 Click **OK** until you have closed all of the Java Control Panel dialog boxes.

Accessing the console

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

Note: Symantec Scan Engine no longer supports accessing the console through a HTTP server.

When you log on to the console, the password for the virtual administrative account is not encrypted. For security reasons, access the console using a switch or a secure segment of the network.

See "About the built-in HTTPS server" on page 53.

You do not need to restart Symantec Scan Engine after you modify a configuration setting for the changes to take effect. Most settings take effect when you apply them. If the Symantec Scan 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 reestablish 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 Scan 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. If the browser session continues to run, you return to the page that you were on when you logged off or when the session times-out.

Only one user should use the console at a time to avoid possible race conditions and configuration change conflicts.

To access the console

1. Launch a Web browser on any computer on your network that can access the server that is running Symantec Scan Engine.
2. In a Web browser, type the following address:

   https://<servername>:<port>/

   where <servername> is the host name or IP address of the server that is running Symantec Scan Engine and <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 Security Alert dialog box appears, click **Yes** to confirm that you trust the integrity of the applet, and then click **Yes** to display the Web page.
4. In the Enter Password box, type the password for the administrative account.
5. Press **Enter**.

About the console

Figure 2-1 shows the Symantec Scan Engine Home page.

Figure 2-1 Symantec Scan Engine Home page

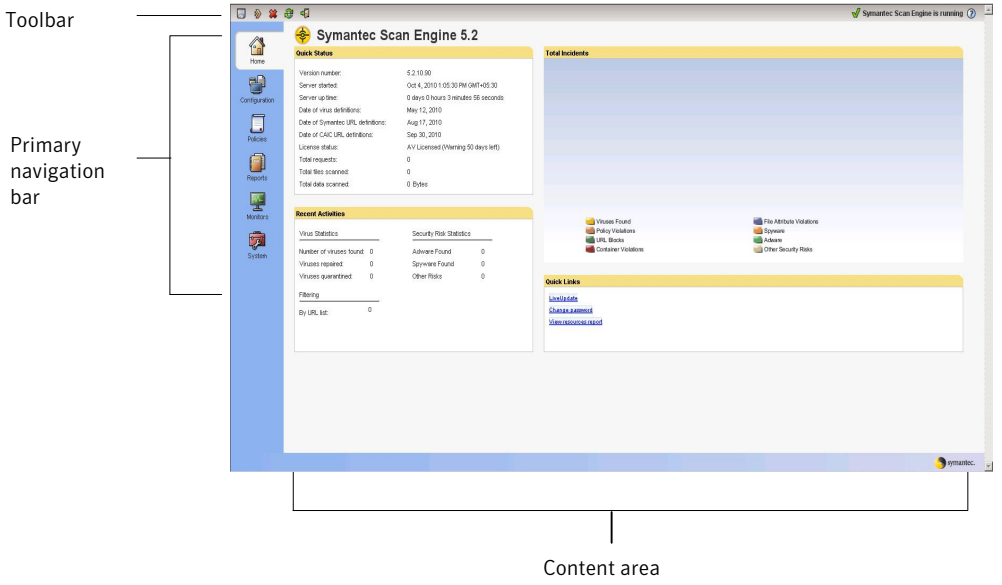
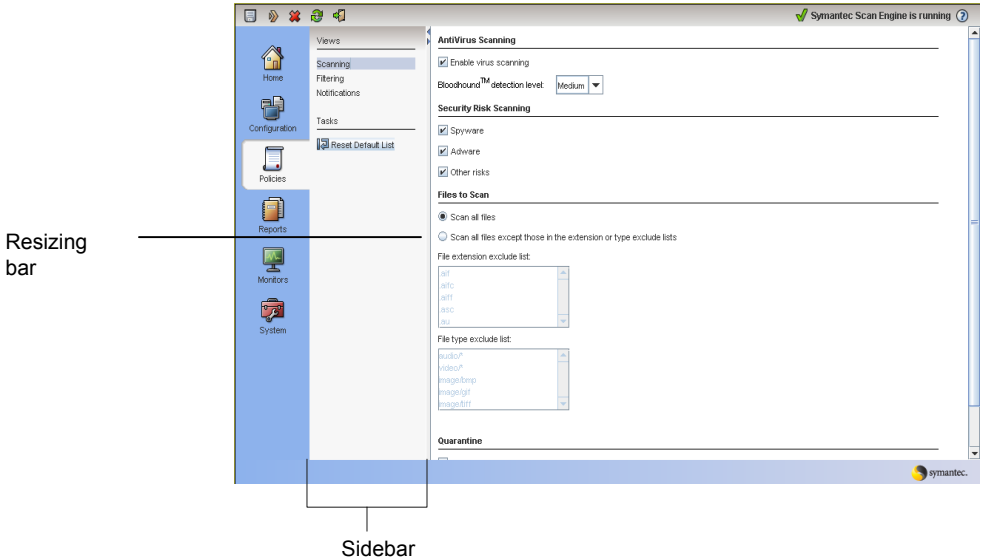


Figure 2-2 shows other console elements.

Figure 2-2 Other console elements



Management operations are grouped into the following categories on the primary navigation bar:

Home	Shows the recent activity and system metrics that are calculated since the last restart.
Configuration	Use to configure Symantec Scan Engine to provide scanning for client applications and set limits to protect server resources.
Policies	Use to specify scanning policies for mail, file properties, URL filtering, and antivirus scanning. You can also configure custom user messages.
Reports	Use to examine scanning statistics, load statistics, logging status, and log data.
Monitors	Use to configure logging and alerting options, outbreak management, and monitor scan requests.
System	Use to perform the following actions: ■ Manage the Symantec Scan Engine administrator account ■ Install new license keys ■ Check the status of the license keys that are installed ■ Update definitions

Use the toolbar icons in the Symantec Scan Engine console to perform the following actions:

Save	Saves your changes to the XML configuration files. Your changes are saved but Symantec Scan Engine does not implement them until you apply the changes. You can continue to make changes to the Symantec Scan Engine configuration through the console.
Apply	Applies all of your changes. Some changes can be applied without restarting Symantec Scan Engine. Other changes do not take effect until the service is restarted. When you click "Apply," you initiate the necessary actions to apply all of the changes. You are prompted to perform a manual restart if one is necessary.
Cancel	Returns the configuration settings to the values that you last saved.
Refresh	Refreshes the display.

Logoff	Logs you out of Symantec Scan Engine.
Help	Opens the online help file.

The toolbar also displays messages about the status of Symantec Scan Engine and any pending changes that need to be saved.

The "Changes pending" message indicates that during the session, you have interacted with the console in some way. "Changes pending" does not necessarily mean that you have made modifications to any settings. For example, if you enable an option and then immediately disable it, "Changes pending" appears on the toolbar. "Changes pending" also appears if you click a drop-down menu to view the available options, but you do not select a different option.

About the built-in HTTPS server

The built-in HTTPS server provides the console for Symantec Scan Engine. It 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 Scan 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 53.

Enhancing security for the HTTPS servers and SSL servers

Symantec Scan 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 Scan 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 54.

See "Forcing Symantec Scan Engine to generate new keys" on page 55.

Importing keys from a third-party certificate

When you install Symantec Scan 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 Scan Engine supports importing PFX and PKCS#12 certificate files.

See "Migrating to version 5.2.11" on page 64.

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 Scan Engine installation directory. The default installation directories are as follows:

Windows	C:\Program Files\Symantec\Scan Engine
Linux and Solaris	/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 Scan Engine 5.2.11 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 Scan 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 Scan Engine installation directory. The default installation directories are as follows:

Windows	C:\Program Files\Symantec\Scan Engine
Linux and Solaris	/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 <SSE Dir>** where <PFX/PKCS#12 certificate file name> is the name of the certificate that you want to import, and <SSE Dir> is the Symantec Scan 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**

Forcing Symantec Scan 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 Scan Engine to generate new keys. When you

delete the existing keystore, Symantec Scan Engine automatically creates new keys the next time you start the Symantec Scan Engine service.

To force Symantec Scan Engine to generate new keys

1. Stop the Symantec Scan Engine service.
2. In the installation directory, delete the following files:

   keyStore.private

   keyStore.public
3. Restart the Symantec Scan Engine service.

See "Verifying, stopping, and restarting the Symantec Scan Engine service on Windows" on page 47.

See "Verifying, stopping, and restarting the Symantec Scan Engine daemon on Linux and Solaris" on page 46.

Changing the administrator settings

Table 2-1describes the administrator settings that you can configure.

Table 2-1 Administrator settings

Option	Description
New password	You manage Symantec Scan Engine by using a virtual administrative account. The virtual administrative account is known only to Symantec Scan Engine. It is not a system account. You are prompted to provide a password for this account at installation. You can change the password for this account through the Symantec Scan Engine console. Remember the password that you enter for this account. The virtual administrative account is the only account that you can use to manage Symantec Scan Engine. If you forget the password for the virtual administrative account, clear the adminpassword variable in the configuration file. Then perform a manual restart of Symantec Scan Engine and log on to the console to enter a new password. (You are not required to have a password when you log on.) See "Editing the Symantec Scan Engine configuration files" on page 219.
Confirm	Type the password again to confirm it.

Table 2-1 Administrator settings *(continued)*

Option	Description
Administrator server address	You manage Symantec Scan 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. **Note:** If you change the administrator server address 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 administrator address.
Administrator port number	The Web-based interface binds to a TCP/IP port number. You are prompted to provide an administrator port number during installation. You can change the port number through the console. If you change the administrator 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:** 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.
SSL port	Symantec Scan 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. **Note:** You must close and reopen the console for the new SSL port setting to take effect.
Administrator timeout	By default, Symantec Scan Engine is configured to automatically log off the administrator after a period of inactivity. The default period of inactivity is 300 seconds (five minutes). You can change the default time-out period. The minimum value is 60 seconds. **Note:** You must close and reopen the console for the new timeout interval setting to take effect.

To change the administrator settings

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

3. In the content area under Administrator Password, in the New password box, type the new password for the virtual administrative account.
4. In the Confirm box, type the new password again to confirm it.
5. Under Administrator Settings, in the Administrator server address box, type a bind address, if necessary.

   By default, Symantec Scan Engine binds to all interfaces. Specify the appropriate bind address to restrict administrative access.
6. In the Administrator 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 Scan 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 Scan Engine by editing the configuration file.

   See "Editing the Symantec Scan Engine configuration files" on page 219.
7. In the SSL port 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 Scan Engine and that is between 1024 and 65535. Do not use port number 80 or port 443.
8. In the Administrator timeout box, type the period of inactivity, in seconds, after which the administrator 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).
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.

You must close and reopen the console for the changes to the administrator settings (except the Administrator Server address) to take effect.

Allocating resources for Symantec Scan Engine

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

Table 2-2 describes the resource settings.

Table 2-2 Resource settings

Option	Description
Temporary directory for scanning	Symantec Scan 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. Scan engine performance depends on this directory being able to accommodate a large volume of data during periods of peak use. The file directory that you specify must already exist. Symantec Scan Engine validates the existence of the directory when you save or apply your changes. The default temporary directories are as follows: ■ Linux and Solaris: <Installdir>/temp ■ Windows: <Installdir>\temp

Table 2-2 Resource settings *(continued)*

Option	Description
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 Scan 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 Scan Engine. Symantec Scan 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 "Controlling the dynamic thread pool" on page 225. **Note:** If you use the RPC protocol and support multiple RPC clients, Symantec Scan 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 2-2 Resource settings *(continued)*

Option	Description
Threshold number of queued requests	Symantec Scan Engine is at maximum load when the number of queued requests exceeds the specified threshold. You can configure Symantec Scan Engine to log the event to the specified logging destinations when the queue exceeds the maximum load. See "Logging levels and events" on page 159. When the ICAP threshold notification feature is enabled (default value), Symantec Scan 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 Scan 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 Scan 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.

Table 2-2 Resource settings *(continued)*

Option	Description
Log or send alert for maximum load every _ minutes	Symantec Scan 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 Scan 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). See "What's new" on page 14. ■ You enable SMTP alerts. ■ You configure "Log or send alert for maximum load every __ minutes." Symantec Scan 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 170.
In-memory file processing	Symantec Scan 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 Scan 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.

Configure the client antivirus software to avoid all scans of the Symantec Scan Engine temporary directory (for example, real-time scans, manual scans, and scheduled scans). This reconfiguration prevents the client software from scanning files before they are sent to Symantec Scan Engine for scanning.

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

The default setting is 128. The maximum recommended value is 512.

5 In the Threshold number of queued requests box, type the threshold number of queued requests that Symantec Scan 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 128 MB. The maximum setting is 2048 MB (2 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 16 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 5.2.11

Table 2-3 describes the upgrades that Symantec Scan Engine supports.

Table 2-3 Supported upgrades

Prior version number	Description
5.2	You can install the upgrade over the existing installation. When you upgrade from version 5.2, Symantec Scan Engine retains all of the settings and values that you have configured.
5.1	You can install the upgrade over the existing installation. When you upgrade from version 5.1, Symantec Scan Engine retains all of the settings and values that you have configured.
4.3x	You can install the upgrade over the existing installation. When you install the upgrade over the current installation, the program retains most of your settings and customizations. Some exceptions apply. See "About migrating from version 4.3x" on page 65.
4.0 and earlier	Upgrades from version 4.0 or earlier of the product are not supported. If you want to upgrade a version 4.0 or earlier installation, you must first upgrade your installation to version 4.3 (which does support a direct upgrade from version 4.0), and then upgrade the version 4.3 installation to version 5.2.11.

Note: Symantec Scan Engine does not support upgrades from version 5.0.

You must stop the Symantec Scan Engine service before you upgrade the software. If you cancel the upgrade on Solaris after selecting the upgrade type, you must reinstall the previous version.

See "Verifying, stopping, and restarting the Symantec Scan Engine service on Windows" on page 47.

If you are upgrading from version 5.2/5.1 and use security certificates, take the following actions:

- If you use the default security files that Symantec Scan Engine generated, delete the keystore.public and keystore.private before you perform the upgrade installation.

- If you use custom security files, you can retain the custom security files. Symantec Scan Engine automatically uses the existing files when you upgrade.

See "Importing keys from a third-party certificate" on page 54.

About retaining the service account when you upgrade to version 5.2.11

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 Scan Engine automatically populates the service account name (non-editable) in the **Symantec Scan 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 Scan 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 Scan Engine Service Credentials** screen appears only if the previous version of Symantec Scan Engine runs on the account other than Local System.

About migrating from version 4.3x

If you are migrating from version 4.3x, consider the following items:

- The ArchiveTypes setting from version 4.3 is not preserved. Instead, the DecEngines setting in version 5.2.11 uses a default value.
- Exclusion lists are not upgraded. For security reasons, changes were made to the default exclusion list.
- Version 5.2.11 does not support inclusion lists.
- Domain blocking settings are not preserved, and the syntax of the entries has changed. The previous settings are saved into an upgrade folder in the installation directory for review and re-entry by the user in the new format.
- If the LiveUpdate interval in Symantec Scan Engine 4.3 is set to a value that is not supported in Symantec Scan Engine 5.2.11, then the interval is reset to every 2 hours.
- Upgrades on Linux and Solaris run under the configured user of the previous installation. To change the user that Symantec Scan Engine runs as, uninstall the existing installation, and perform a clean installation of version 5.2.11. The installation user interface asks what (non-root) user you want Symantec Scan Engine to run as.

- Symantec Scan Engine tries to use port 8005 after an upgrade for the Secure Socket Layer (SSL). If that port is in use, manually change the SSL port to an available port number. Then restart the Symantec Scan Engine.
  See "About the built-in HTTPS server" on page 53.
- If you upgrade from version 4.3.7 or later, the maximum file size settings are not preserved. The maximum file size threshold is automatically set to 2,147,483,648 bytes (2 GB).

Table 2-4 provides information about how the configuration files are affected after an upgrade from version 4.3x.

Table 2-4 Configuration files that are affected after an upgrade

File or message catalog	Description
Symcscan.cfg	This file is no longer used. This data is now stored in a set of XML files. During the upgrade, any changes that you made to the Symantec Scan Engine configuration file, Symcscan.cfg, are preserved. If you have customized any configuration options, the data is copied during the upgrade to the appropriate XML file. A command-line configuration modifier tool is available for changing the configuration values in the XML files. See "About the Symantec Scan Engine command-line scanner" on page 201. **Note:** Logging options have changed. Some of the previous configuration options do not map to the new options. Therefore, some customizations that you have made to the logging options are not preserved. You might need to reconfigure your logging options after you install the upgrade.
Policy.cfg, Subjects.cfg, Sizes.cfg, and Filenames.cfg	These files are not used in version 5.2.11. This data is now stored in a set of XML files. During the upgrade, any changes that you have made to these files are preserved. If you have customized any options, the data is copied during the upgrade to the appropriate XML file. Several of the settings that are contained in these files now apply to all files, rather than to mail files only. If you had a mail policy in effect, check the configuration through the Symantec Scan Engine console after the upgrade is complete.

Table 2-4 Configuration files that are affected after an upgrade *(continued)*

File or message catalog	Description
Domains.cfg	This file is not used in version 5.2.11. This data is now stored in a set of XML files. During the upgrade, any changes that you have made to this file are not preserved because of a syntax incompatibility with wildcard characters. You must reconfigure the blacklist (blocking by message origin) after the upgrade is complete. **Note:** The Domains.cfg file is not removed during the upgrade. The file is retained so that you can refer to the file to reconfigure the blacklist after the upgrade.
Symcsmsg.dat	This file is not used in version 5.2.11. Message string data is stored in a set of XML files. If you have customized any of the message strings in the message string file, the customizations are not retained. During the upgrade, the message strings revert to the default text. **Note:** Some customization options that were allowed in previous versions are no longer available. The logging and alert messages that you can customize are available through the console.
Symcsinf.htm and Symcsinf.msg (ICAP only)	Customized ICAP access denied messages are not retained.
Existing local logs	Existing local log files are retained. The logs in version 5.2.11 use a different format. Data from previous log files are not included in the reports that are generated in version 5.2.11.
filtering.xml	All DDR-related tags have been removed. The permissible value for `FilteringMode` parameter has been changed and a new parameter `EnableFilteringAndDownloadDefinitions` has been added to the file. The `Locale` parameter has been removed.

Uninstalling Symantec Scan Engine

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

the license keys. You must also manually uninstall the license files for Symantec Scan Engine.

See "About removing license files" on page 73.

When you uninstall Symantec Scan 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 53.

To uninstall Symantec Scan 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 Scan Engine**.
3. Click **Remove**.
4. Follow the on-screen instructions to complete the uninstallation.

To uninstall Symantec Scan Engine on Solaris

1. Login to the computer as root.
2. At the command prompt, type the following command:

   pkgrm SYMCScan
3. Follow the on-screen instructions to complete the uninstallation.

To uninstall Symantec Scan Engine on Linux

1. Login to the computer as root.
2. At the command prompt, type the following command:

   rpm -e SYMCScan

Chapter 3

Activating licenses

This chapter includes the following topics:

- About licensing
- About license activation

About licensing

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

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

Product licenses	Product licenses activate scanning functionality. The AV Scanning license activates the threat scanning features and security risk scanning features. The URLFiltering license activates the HTTP URL filtering features. See "About scanning for risks" on page 95. See "About categories" on page 134.
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. See "About definition updates" on page 179.

You must have valid product licenses to configure the product and to access the threat (antivirus), security risk, 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.

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

Symantec Scan Engine installs with the most current definitions that are available at the time the product is released. After you install the product and active 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 192.

When a license is within 60 days of its expiration date, it is considered to be in a warning period. After a license expires, the licensed feature continues to operate for a specified period of time. This specified period of time is the grace period. If the grace period expires with no license renewal, all record of the license is removed. To regain product functionality when your license expires, you must renew and reactivate your license subscription.

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

See "About logging data" on page 157.

See "Checking the license status" on page 73.

About license activation

You activate scanning features and definitions updates for Symantec Scan 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 Scan 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 Scan 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 71.

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 71.
Install the license file.	You must install the content licenses and product licenses on each server on which you run Symantec Scan 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 72.

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 26.

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 26.

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 71.

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.

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 Scan 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:

- When you receive the email message from Symantec that contains the license file, do one of the following steps:
  - In Windows, save the license file in the following location: C:\Program Files\Common Files\Symantec Shared\Licenses
  - In Solaris or Linux, save the license file in the following location: /opt/Symantec/Licenses

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

About removing license files

The license files for Symantec Scan 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:\Program Files\Common Files\Symantec Shared\Licenses
Linux and Solaris	/opt/Symantec/Licenses

Checking the license status

You can view information about the status of your Symantec Scan Engine licenses. You can check the license expiration date and the number of days that remain in the warning or grace period (if applicable).

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

Table 3-1 License status information

Column	Description
Feature	This column lists each license that is installed.
Expiration	This column lists the expiration date for each license. If the license is in the warning period or the grace period, a warning message is displayed in this column.
Fulfillment ID	The fulfillment ID is the identification number for your license. You must provide this number to Symantec Technical Support if you have questions about your license.

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

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.

Chapter 4

Configuring scanning services for client applications

This chapter includes the following topics:

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

About the communication protocols

You can select the communication protocol that Symantec Scan 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 Scan Engine uses ICAP by default. ICAP is a lightweight protocol for executing a remote procedure call on HTTP messages. Symantec Scan Engine supports version 1.0 of ICAP, as presented in RFC 3507 (April 2003). See "About working with ICAP" on page 79.

Symantec Scan Engine native protocol	Symantec Scan Engine includes its own native protocol. The native protocol is a TCP/IP protocol. It is text-based like HTTP or SMTP. It uses ASCII commands and responses to communicate between the client and the server. See "Working with the native protocol" on page 82.
Remote procedure call (RPC)	If you use Windows, you can use a proprietary scanning protocol with the MS-RPC protocol to interface with client applications. This option is not available for Solaris or Linux. See "Working with the RPC protocol" on page 84.

Supported services by protocol

The services that are available through Symantec Scan 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

Feature	Internet Content Adaptation Protocol (ICAP)	Native protocol	RPC protocol
Threat detection See "Enabling threat detection" on page 97.	Supported	Supported	Supported
Security risk detection See "Enabling security risk detection" on page 100.	Supported		Supported
Container processing limits See "Setting container file limits" on page 129.	Supported	Supported	Supported
Partial and encrypted malformed MIME detection See "Configuring Symantec Scan Engine to block unscannable container files" on page 103.	Supported	Supported	Supported

Table 4-1 Supported services by protocol *(continued)*

Feature	Internet Content Adaptation Protocol (ICAP)	Native protocol	RPC protocol
File name filtering See "Configuring file name filtering" on page 105.	Supported	Supported	
File or attachment size filtering See "Configuring file size filtering" on page 107.	Supported	Supported	
Scanning by file extension and file type See "Specifying which files to scan" on page 125.	Supported	Supported	Supported
Scanning by file size See "Specifying the maximum file or message size to scan" on page 128.	Supported	Supported	
Message origin filtering See "Configuring message origin filtering" on page 110.	Supported	Supported	
Subject line content filtering See "Configuring subject line content filtering" on page 108.	Supported	Supported	
Quarantining infected files See "Quarantining infected files that cannot be repaired" on page 99.	Supported		Supported
HTTP content filtering See "How to filter a URL" on page 148.	Supported		

Table 4-1 Supported services by protocol *(continued)*

Feature	Internet Content Adaptation Protocol (ICAP)	Native protocol	RPC protocol
Logging events to the following destinations: ■ Local logs See "About configuring local logging" on page 163. ■ Windows Application Event Log See "Configuring logging to the Windows Application Event Log" on page 168. ■ Statistics Log See "Enabling statistics reporting" on page 167. ■ Symantec Security Information Manager See "Configuring Symantec Scan Engine to log events to SSIM" on page 169. ■ Abort log See "Logging destinations" on page 157.	Supported	Supported	Supported
RPC client logging See "Logging to the RPC client logging subsystem" on page 91.			Supported
Monitor scanning requests See "Monitoring scanning requests" on page 115.	Supported	Supported	Supported
Continuous self-test scanning See "Disabling automatic self-test scanning" on page 233.	Supported		Supported

Table 4-1 Supported services by protocol *(continued)*

Feature	Internet Content Adaptation Protocol (ICAP)	Native protocol	RPC protocol
Notification to the ICAP client that the queued requests threshold is reached See "Allocating resources for Symantec Scan Engine" on page 59. See "Disabling the ICAP threshold client notification" on page 227.	Supported		
SMTP and SNMP alert and outbreak notifications See "About configuring alerts" on page 170.	Supported	Supported	Supported
Command-line scanning See "About the Symantec Scan Engine command-line scanner" on page 201.	Supported		

About working with ICAP

In its default configuration, Symantec Scan 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 Scan Engine to request scanning services.

The Symantec Scan 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 URL scanning to any C, C++, Java, or .Net application.

When you use ICAP as the communication protocol, Symantec Scan Engine initially provides information to the ICAP client about which file types to scan. This information is based on the configuration of Symantec Scan Engine.

If the file extension is one that is identified for scanning, the ICAP client forwards the entire file to Symantec Scan 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 Scan 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 Scan Engine might request and scan a file even when it is not identified for scanning.

Symantec Scan 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 Scan 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 ICAP-specific options. You must also configure the ICAP client to work with Symantec Scan Engine. For more information, see the ICAP client documentation.

Table 4-2 describes the configuration options for ICAP.

Table 4-2 Protocol-specific options for ICAP

Option	Description
Bind address	Symantec Scan Engine detects all of the available IP addresses that are installed on the host. By default, Symantec Scan 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 Scan 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 Scan Engine binds to all of the scanning IP addresses that it detects. If Symantec Scan 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 Scan 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 159. **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 Scan Engine.

Table 4-2 Protocol-specific options for ICAP *(continued)*

Option	Description
Port number	The port number must be exclusive to Symantec Scan Engine. You must use the same port number for all of the scanning IP addresses that you want to bind to Symantec Scan 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.
Scan policy	Symantec Scan Engine can handle a file that contains a risk in one of the following ways: ■ Scan only Denies 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.

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 Scan Engine service.

   See "Verifying, stopping, and restarting the Symantec Scan Engine service on Windows" on page 47.

5 Under ICAP Configuration, in the Bind address table, select the scanning IP addresses that you want to bind to Symantec Scan 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 Scan 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 Scan 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 Scan Engine.

7 In the Scan policy list, select how you want Symantec Scan Engine to handle infected files.

The default setting is Scan and repair or delete.

8 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.

Working with the native protocol

Symantec Scan Engine implements a TCP/IP protocol to provide scanning functionality to client applications. It is text-based like HTTP or SMTP. It uses ASCII commands and responses to communicate between the client and the server. To submit a file for scanning, a client connects to the specified IP port and sends the file to Symantec Scan Engine to be scanned. Symantec Scan Engine scans the file and sends the results to the client. After the client receives these results, the connection is closed. The client opens a new connection for each file that it sends to Symantec Scan Engine.

Configuring native protocol options

If you select the native protocol, you must configure certain protocol-specific options.

Table 4-3 describes the configuration options for the native protocol.

Table 4-3 Protocol-specific options for the native protocol

Option	Description
Bind address	By default, Symantec Scan Engine binds to all interfaces. You can restrict access to a specific interface by entering its bind address. You can use 127.0.0.1 (the loopback interface) to let only the clients that run on the same computer connect to Symantec Scan Engine.
Port number	The port number must be exclusive to Symantec Scan Engine. The default port number is 7777. If you change the port number, use a number that is greater than 1023. No other program or service should use this port number.
Local scan directory	You only need to provide a local scan directory when the client application and Symantec Scan Engine run on the same computer. The client application passes the file name to Symantec Scan Engine. Symantec Scan Engine opens the file and scans it in the local scan directory that you specify. The directory that you specify must already exist. If you do not specify a local scan directory, Symantec Scan Engine stores files and scans them in the temporary directory for virus scanning. See "Allocating resources for Symantec Scan Engine" on page 59. **Note:** If the computer is running the client version of an antivirus software product, you must configure the client product to exclude the local scan directory from all types of scanning (for example, real-time scans, scheduled scans, and manual scans).

If you use Windows and you change the protocol setting to the native protocol, you might need to change the service startup properties to identify an account that has sufficient permissions to run Symantec Scan Engine.

See "Editing the service startup properties" on page 92.

To configure native protocol 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 **Native**.

4 In the Manual Restart Required dialog box, click **OK**.

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

5 Under Native Protocol Configuration, in the Bind address box, type a bind address, if necessary.

By default, Symantec Scan Engine binds to all interfaces. You can restrict access to a specific interface by typing its bind address. 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 Scan Engine.

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

The default setting is port 7777. If you change the port number, use a port number that is equal to or greater than 1024. No other program or service should use this port number.

7 In the Local scan directory box, type a local scan directory path, if necessary.

The file directory that you specify must already exist. Symantec Scan Engine validates the existence of the directory when you save or apply your changes.

If you do not specify a local scan directory location, Symantec Scan Engine uses the temporary directory for scanning.

See "Allocating resources for Symantec Scan Engine" on page 59.

8 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.

Working with the RPC protocol

You can configure Symantec Scan Engine to use the RPC protocol to interface with appropriate clients. To use the RPC protocol, Symantec Scan Engine must be installed on a computer that is running Windows 2000 Server/Windows 2003 Server/Windows 2008 Server. It must also be located in the same domain as the RPC clients for which it provides scanning and repair services. A single scan engine

can support multiple RPC clients. For sites with larger scan volumes, multiple scan engines also can be used to support one or more RPC clients.

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

See "Verifying, stopping, and restarting the Symantec Scan Engine service on Windows" on page 47.

About RPC configuration options

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

Table 4-4 describes the configuration options for RPC.

Table 4-4 Protocol-specific options for RPC

Option	Description
RPC client list	A single Symantec Scan Engine can support multiple RPC clients. Clients must be located in the same domain as Symantec Scan Engine. You must provide the IP address of each RPC client. See "Adding and removing RPC clients" on page 87.
Check RPC connection every __ seconds	Symantec Scan Engine maintains a connection with the RPC client. You can configure Symantec Scan 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 RPC connection options" on page 88.
Maximum number of reconnect attempts	You can limit the number of times Symantec Scan Engine tries to re-establish a lost connection with the RPC client. If the client does not respond within this limit, Symantec Scan Engine stops trying to reestablish a connection. By default, Symantec Scan Engine tries to reconnect with the RPC client indefinitely. **Note:** Do not set a maximum number of reconnect tries if Symantec Scan Engine provides scanning for multiple RPC clients. See "Configuring RPC connection options" on page 88.

Table 4-4 Protocol-specific options for RPC *(continued)*

Option	Description
Antivirus scan policy	Symantec Scan Engine can handle a file that is infected in one of the following ways: ■ Scan only Denies access to the infected file but does nothing to the infected file. ■ Scan and repair files Tries to repair infected files and denies access to any unrepairable files. ■ Scan and repair or delete Tries to repair infected files and deletes any unrepairable files from archive files. **Note:** You must select "Scan and repair or delete" to quarantine the infected files that cannot be repaired. See "Configuring the RPC scanning policy" on page 89.
Automatically send antivirus update notifications	Symantec Scan Engine can automatically notify the RPC client that Symantec Scan Engine has new definitions. This notification prompts the RPC client to clear its cache of scanned files. See "Notifying a file server when definitions are updated" on page 90.

Configuring Symantec Scan Engine to use the RPC protocol

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

To configure Symantec Scan 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 Scan 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.

Adding and removing RPC clients

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

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 Scan 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 RPC connection options

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

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 Scan 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 Scan Engine should try to re-establish a lost connection with the RPC client.

The default setting is 0, which causes Symantec Scan Engine to try indefinitely to reestablish a connection. Use the default setting if Symantec Scan 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.

Configuring the RPC scanning policy

You can specify how you want Symantec Scan Engine to process the files that are infected.

To configure the RPC scanning policy

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 Antivirus scan policy list, select one of the following:

Scan only	Denies access to the infected file but does nothing to the infected file.
Scan and repair files	Tries to repair infected files and denies access to any unrepairable files.
Scan and repair or delete	Tries to repair infected files and deletes any unrepairable files from archive files. This is the default setting.

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.

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 Scan Engine for scanning. When Symantec Scan 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 Scan Engine to automatically notify the RPC client that Symantec Scan 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 Scan 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 Scan 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. 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, check **Automatically send antivirus update notifications**.

   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**.

Logging to the RPC client logging subsystem

Certain Symantec Scan 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

User identification and notification when a risk is found

When Symantec Scan Engine finds a risk in a file that a RPC network-attached-storage client requests, Symantec Scan 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 Scan Engine. This feature provides administrators with as much information as possible when a risk is found.

Note: Symantec Scan Engine can obtain only the information that the RPC client makes available. If the identification information is available, Symantec Scan 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.

You also can configure Symantec Scan Engine to notify the requesting user that the retrieval of a file failed because a risk was found. The notification message only displays if the user is running Windows.

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 114.

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

See "Editing the service startup properties" on page 92.

Editing the service startup properties

If Symantec Scan 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 Scan 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 Scan Engine runs

- Rights to run as a service

If your client uses the native protocol, the account that you assign to the Symantec Scan Engine service must have access rights to any shared drives or universal naming convention (UNC) paths for which you want to provide scanning services. This account should also have Change permission so that Symantec Scan Engine can delete the infected files that it cannot repair.

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 Scan 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 Scan Engine runs.

   Use the following format for the account name:

   domain\username
6. Click **OK**.
7. Stop and restart the Symantec Scan Engine service.

   See "Verifying, stopping, and restarting the Symantec Scan Engine service on Windows" on page 47.

Chapter 5

Protecting against risks

This chapter includes the following topics:

- About scanning for risks
- Enabling threat detection
- Enabling security risk detection
- About preventing potential threats
- Customizing user notifications

About scanning for risks

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

Symantec Scan Engine can detect the following types of risks:

- Threats (such as viruses, worms, and Trojan horses)
  See "Enabling threat detection" on page 97.
- Security risks (such as adware and spyware)
  See "Enabling security risk detection" on page 100.
- Denial-of-service attacks
  See "Setting container file limits" on page 129.

Symantec Scan 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" on page 102.

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 "Configuring Symantec Scan Engine to block unscannable container files" on page 103.

See "Specifying which files to scan" on page 125.

See "Specifying the maximum file or message size to scan" on page 128.

For more information about 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

How Symantec Scan Engine detects risks

Symantec Scan Engine uses the following tools to detects 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 Scan Engine scans for risks, it searches for these signatures.
Heuristics	Symantec Scan 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 Scan 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 Scan 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 Scan Engine scans a file and its contents until it reaches the maximum depth that you specify. Symantec Scan 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 Scan Engine resumes scanning any remaining files. This process continues until Symantec Scan Engine scans all of the files to the maximum depth (that do not meet any of the processing limits).

Enabling threat detection

Symantec Scan Engine can detect threats, such as viruses, Trojan horses, and worms 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 Scan Engine console.

Symantec Scan 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. A high level of protection increases protection of your network; however, server performance might be affected. At lower levels of protection, an unknown threat might escape detection, but system performance decreases. In most cases, the default setting (medium) is appropriate.

See "How Symantec Scan Engine detects risks" on page 96.

See "Ways to test threat detection capabilities" on page 98.

To enable 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 Antivirus Scanning, check **Enable virus scanning**.

4 In the Bloodhound detection level drop-down list, select the appropriate Bloodhound detection level as follows:

Off	Disables antivirus scanning.
Low	Optimizes server performance, but might not detect potential threats.
Medium	Provides a balance between threat detection and server performance. This is the default setting.
High	Increases the detection of threats, but might impact server performance.

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.

Ways to test threat detection capabilities

You can test the threat detection capabilities of Symantec Scan 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.

Quarantining infected files that cannot be repaired

When you use the ICAP protocol or the RPC protocol, you can quarantine infected files (files that contain threats) that cannot be repaired. To quarantine infected files, you must install Symantec Central Quarantine.

Note: Files that contain security risks cannot be quarantined.

See "Enabling security risk detection" on page 100.

Symantec Central Quarantine must be installed on a computer that runs Windows 2000 Server/Windows 2003 Server/Windows 2008 Server. Symantec Central Quarantine and its product manual are included on the Symantec Scan Engine CD.

For more information, see the *Symantec Central Quarantine Administrator's Guide*.

Symantec Scan Engine forwards the infected files that cannot be repaired 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 infected 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 scan policy to forward files to the quarantine. When a copy of an infected file is forwarded to the Symantec Central Quarantine, if the original, infected file can be repaired, it is repaired. If it cannot be repaired, it is deleted.

Note: If your client uses RPC and the submission to the Central Quarantine fails, the disposition of the original file depends on where the file resides. If the file is on the disk, it is deleted. If it is in memory, a replacement is sent over the network to the client.

If you plan to quarantine infected files that cannot be repaired, configure Symantec Scan Engine to quarantine infected files. Also provide the host name or IP address for the computer on which Symantec Central Quarantine server is installed.

To quarantine infected files that cannot be repaired

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 Quarantine, check **Quarantine files**.

4 In the Central server quarantine 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 Scan Engine uses to pass files to Symantec Central Quarantine.

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.

Enabling security risk detection

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

Security risks are 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

Security risks 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

Table 5-1 lists the categories of security risks that Symantec Scan Engine detects.

Table 5-1 Security risk categories

Category	Description
Spyware	Stand-alone programs that can secretly monitor system activity and detect passwords and other confidential information and then relay the information back to a remote computer.
Adware	Programs that gather personal information through the Internet and relay it back to a remote computer without the user's knowledge. Adware might monitor browsing habits for advertising purposes. It can also deliver advertising content.
Other risks	Other risks include the following: ■ Hacking tools Programs that are used to gain unauthorized access to a user's computer. For example, a keystroke logger tracks and records individual keystrokes and sends this information to a remote computer. The remote user can perform port scans or vulnerability scans. Hacking tools might also be used to create viruses. ■ Dialers Programs that use a computer, without the user's permission or knowledge, to dial out through a modem to a 900 number or FTP site, typically to accrue charges. ■ Joke programs Programs that alter or interrupt the operation of a computer in a way that is intended to be humorous or bothersome. For example, a joke program might move the Recycling Bin away from the mouse when the user tries to click on it. ■ Remote access programs Programs that allow a remote user to gain access to a computer over the Internet to gain information, attack, or alter the host computer. ■ Trackware Applications that trace a user's path on the Internet and relay the information to a remote computer.

Symantec Scan Engine scans for security risks in all types of content, such as email messages and Web content. Symantec Scan Engine can also scan POST transactions for security risks. Symantec Scan Engine can only perform security risk scanning when you enable virus scanning.

See "Enabling threat detection" on page 97.

If a security risk is detected, Symantec Scan Engine applies the scan policy that you configured for ICAP; however, security risks cannot be repaired. Files that contain only security risks cannot be quarantined.

See "Configuring ICAP options" on page 80.

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

See "About licensing" on page 69.

To enable security risk 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 Security Risk Scanning, check the security risks that you want Symantec Scan Engine to detect.

   Security risk options are only available if virus scanning is enabled. When you enable virus scanning, all of the security risk options are enabled 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.

About preventing potential threats

Symantec Scan Engine has features you can use to prevent emerging threats by doing the following:

Block unscannable container files	Use this feature to block certain types of unscannable container files, such as partial container files, that might contain threats or malicious code. See "Configuring Symantec Scan Engine to block unscannable container files" on page 103.

Block or delete files by file name	Use this feature to filter documents by file name. See "Configuring file name filtering" on page 105.
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" on page 107.
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" on page 108.
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" on page 110.

Configuring Symantec Scan Engine to block unscannable container files

You can block container files based on certain criteria that might indicate the presence of a threat or malicious code. You can also block container files that might prevent Symantec Scan Engine from effectively scanning the file.

Table 5-2 describes the types of container files that you can block.

Table 5-2 Settings for container file blocking

Type of file	Description
Partial container files	Symantec Scan 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 Scan Engine for scanning. Symantec Scan Engine is configured by default to reject partial messages because they cannot effectively be scanned for threats.
Malformed container files	Computer viruses and malicious programs sometimes create intentionally malformed files. Symantec Scan Engine recognizes such files. If Symantec Scan Engine can identify the container type, in some cases, it can repair the container file. If Symantec Scan Engine cannot determine the container type, Symantec Scan Engine rejects it as a potentially infected file.
Encrypted container files	Infected files are often encrypted to defect scanning attempts. Encrypted files cannot be decrypted and scanned without the appropriate decryption tool. You can configure Symantec Scan Engine to delete encrypted container files to protect your network from threats.

To configure Symantec Scan Engine to block unscannable 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 containers**.

   By default, Symantec Scan Engine rejects partial container files.
4. Under Malformed Container File Processing, check **Block malformed containers**.

   By default, Symantec Scan Engine rejects malformed container files.

5 Under Encrypted Container Handling, check **Delete encrypted containers**.

Encrypted containers are automatically deleted 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.

Configuring file name filtering

If your client uses the ICAP protocol or the native 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 Scan 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 Scan 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 Scan 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 user notifications" on page 111.

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 native protocol or the antivirus-only application program 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.

To configure file name filtering

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 Scan 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.

Configuring file size filtering

If your client uses the ICAP protocol or the native 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 Scan 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 Scan 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 Scan 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 Scan 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 user notifications" on page 111.

Note: If your client uses the native protocol or the antivirus-only application program 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.

To configure file size filtering

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 Scan 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.
Remove a file size from the list.	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.

Configuring subject line content filtering

If your client uses the ICAP protocol or the native protocol, you can configure Symantec Scan 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 Scan 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 Scan 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 Scan Engine automatically encodes and saves the text strings in Unicode/UTF-8 when you apply your changes in the console.

To configure subject line content filtering

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 \\.
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.

Configuring message origin filtering

If your client uses the ICAP protocol or the native protocol, you can configure Symantec Scan 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$@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@internet.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

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.

Customizing user notifications

You can configure Symantec Scan Engine to customize messages to users to notify them when a file has been infected, repaired, 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 Scan 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 Scan 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 5-3 describes the types of notification messages that you can customize.

Table 5-3 Notification messages

Type of notification	Default text
Deleted file	File: ${FILE_NAME} was infected with ${VIRUS_NAME} ({$VIRUS_ID}). File {$QUARANTINED}. File was deleted
Repaired file	File: ${FILE_NAME} was infected with ${VIRUS_NAME} ({$VIRUS_ID}). File {$QUARANTINED}. File was repaired
Infected file	File: ${FILE_NAME} was infected with ${VIRUS_NAME} ({$VIRUS_ID}). File {$QUARANTINED}. File is still infected
Total viruses found	This email message was infected. ${TOTAL_VIRUSES} number of viruses or security risks were found.
Denied file size	The file attached to this email was removed because the file size is not allowed. File attachment: ${FILE_NAME}. Matched file size: ${FILE_SIZE}.
Denied file names	The file attached to this email was removed because the file name is not allowed. File attachment: ${FILE_NAME}. Matched pattern: ${MATCHING_FILENAME_ENTRY}.
Encrypted file	The encrypted container attached to this email was removed. File attachment: ${FILE_NAME}.
Web browser	The content you just requested contains ${VIRUS_NAME} and was blocked by the Symantec Scan Engine based on local administrator settings. Contact your local administrator for further information.

Table 5-4 lists the variables that you can use to customize your notifications.

Table 5-4 Notification variables

Variable	Description
${FILE_NAME}	The name of the infected file.
${FILE_SIZE}	The size of the file that violates the maximum file size threshold. See "Configuring file size filtering" on page 107.
${VIRUS_NAME}	The name of the threat or security risk.
${VIRUS_ID}	The threat or security risks identification number.
${QUARANTINED}	Indicates whether a file was quarantined.
${TOTAL_VIRUSES}	The total number of risks that are detected in the MIME message.
${MATCHING_ FILENAME_ENTRY}	The file name pattern that triggered the violation. See "Configuring file name filtering" on page 105.

To customize user notifications

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 Scan 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 Scan Engine that detected the infection. For example, the message contains the IP address and the port number of Symantec Scan 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 Scan Engine. The Windows Messenger service must be running both on the computer on which Symantec Scan 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. 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.

Chapter 6

Monitoring and tuning Symantec Scan Engine performance

This chapter includes the following topics:

- How to monitor Symantec Scan Engine performance
- Ways to improve Symantec Scan Engine performance

How to monitor Symantec Scan Engine performance

You should continually monitor Symantec Scan 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 "Ways to improve Symantec Scan Engine performance" on page 121.

You can monitor Symantec Scan Engine performance in the following ways:

- Monitoring Symantec Scan Engine resources
- Monitoring scanning requests

Monitoring scanning requests

Symantec Scan Engine provides a feature that lets you define the expected scanning load for specific time periods. When the Symantec Scan 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 Scan 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 159.

Symantec Scan 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 Scan Engine sends an alert.

For example, if you set a threshold of 20 requests a second for Wednesday from 1:00 A.M. to 2:00 A.M., Symantec Scan Engine does not generate an alert for any minute in which it receives 1,200 requests (20 requests times 60 seconds). Symantec Scan 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.

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 request/second**.
     You must enable the feature to add, activate, deactivate, or delete any schedules.
   - To disable the feature, uncheck **Monitor request/second**.

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 Scan 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.

Monitoring Symantec Scan Engine resources

You can monitor the resources Symantec Scan 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 Scan Engine to appear on the Resources page.

Symantec Scan 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

Item	Description
RPC Client	IP address of the RPC client This setting only applies to the RPC protocol.
Active threads	Number of threads that Symantec Scan Engine uses to perform the scan
Waiting threads	Number of threads that are available for the scanning job
Thread pool size	Maximum number of threads that are available for scanning See "Allocating resources for Symantec Scan Engine" on page 59.

Table 6-2 describes the load statistics resources that you can monitor.

Table 6-2 Load statistics

Item	Description
Threshold for queued requests	Number of scan requests at which Symantec Scan Engine is at maximum load See "Allocating resources for Symantec Scan Engine" on page 59.
Queued requests	Number of scan requests that are currently scheduled or pending
Number of requests per sec	Average of number of scanning requests that arrived in past 60 seconds
Total files scanned	Number of files that Symantec Scan Engine scanned since the program was last restarted
Total data scanned	Total data that Symantec Scan Engine scanned since the program was last restarted

Table 6-3 describes the logging statistics resources that you can monitor.

Table 6-3 Logging statistics

Item	Description
Log directory location	Location of log files See "Allocating resources for Symantec Scan Engine" on page 59.
Used space	Amount of used space for the location in which the Symantec Scan Engine logs are maintained
Available space	Remaining available space for the location in which the Symantec Scan Engine logs are maintained **Note:** This information might be inaccurate if you use Solaris and the directory that Symantec Scan Engine uses for logging is part of a network file share.

Table 6-4 describes the miscellaneous resources that you can monitor.

Table 6-4 Miscellaneous

Item	Description
Process priority	The Symantec Scan Engine process priority For more information about how to change a process priority, see the documentation for your operating system.

To monitor Symantec Scan Engine resources

- Do one of the following steps:
  - In the console on the primary navigation bar, click **Reports**, and then click **Resources**.
  - In the console on the Home page, in the Quick Links pane, click **View resources report**.

Ways to improve Symantec Scan Engine performance

Symantec Scan Engine installs with a default configuration that is designed to balance scanning services with scanning performance. However, you can modify Symantec Scan Engine settings and resources to maximum performance.

See "Deployment considerations and recommendations" on page 122.

See "Enhance performance by limiting scanning" on page 124.

See "Configuration settings that can conserve and enhance performance" on page 131.

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 Scan Engine performance" on page 115.

Deployment considerations and recommendations

Table 6-5 provides the deployment considerations that can improve Symantec Scan Engine performance.

Table 6-5 Symantec Scan Engine deployment recommendations

Deployment consideration	Description
Determining CPU speed and system architecture capacity	Symantec Scan 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 Scan 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 Scan 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 6-5 Symantec Scan Engine deployment recommendations *(continued)*

Deployment consideration	Description
Determining network capacity	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 could be the result of over-utilization of the Internet link. If Symantec Scan 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 Scan Engine servers. You should also ensure that the entire networking infrastructure is appropriately rated. For example, if you connect 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.
Determining disk storage capacity	Symantec Scan 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 Scan Engine. If you experience disk space shortages, consider adding more physical disks.

Enhance performance by limiting scanning

A method that you can use to enhance scanning performance is limiting the files that Symantec Scan Engine scans.

You can limit the files that are scanned as follows:

Exclude specific file extensions and file types from scanning	When you enable this option, Symantec Scan 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 125.
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. This option is available for the ICAP and native protocols only. See "Specifying the maximum file or message size to scan" on page 128.
Impose limits on container files	You can impose limits on how you want Symantec Scan 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 129.

Specifying which files to scan

Threats are only found in the file types that contain executable code. When Symantec Scan 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 files that might contain threats, based upon their file extensions or file types.

Symantec Scan 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 Scan 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/bmp	image/gif
image/tiff	image/x-png	image/x-pixmap
image/x-ico	audio/mtm	audio/x-aiff
audio/x-au	audio/midi	audio/x-wav
audio/x-realaudio	audio/x-mpeg	audio/x-s3m
audio/shn	audio/x-stx	audio/it
audio/x-mod	audio/med	video/x-ms-wmv
video/x-msvideo	video/mpeg	video/quicktime
binary/ms-structured-storage	application/x86-win-32-exe	application/pcx
application/ms-tnef	application/lzh	application/x-lharc
application/x-lha	application/rar	application/lz
application/arj	application/x-gzip	application/ole
application/x-zip	application/x-ace	application/graphicconverter
application/java-archive	application/x-tar	application/cab
application/ani	application/bh	application/x-bz2
application/imz	application/x-macbinary	application/x-ogg
application/x-pdf	application/rtf	application/x-sit
application/x-zoo	application/postscript	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 Scan 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.

Specifying the maximum file or message size to scan

If your client uses the ICAP protocol or the native 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 Scan Engine has no limits on total file or message sizes.

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 Scan Engine should accept.

The default value is 0. This setting places no limits on file or message size.

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.

Setting container file limits

Symantec Scan 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 Scan 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 Scan Engine scans a file and its contents until it reaches the maximum depth that you specify. Symantec Scan 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 Scan Engine resumes scanning any remaining files. This process continues until Symantec Scan 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 permitted 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 Scan 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 Scan 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 When processor limit is met (or exceeded), select whether to allow or deny access to container files for which one or more limits are exceeded.

   Access is denied by default.

7 Under NonMIME threshold, in the No determination after reading box, type the maximum number of bytes that Symantec Scan Engine should scan to determine whether a file is MIME-encoded.

The default setting is 200000 bytes. If Symantec Scan 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.

8 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.

Configuration settings that can conserve and enhance performance

Table 6-6 describes the configurations that you can modify to enhance Symantec Scan Engine performance.

Table 6-6 Configurations to enhance performance

Configuration	Description
Modify system scanning resources	The system scanning resource settings that you can modify to enhance performance are as follows: ■ Temporary directory 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 files to be scanned. Scan engine performance depends on this directory being able to accommodate a large volume of large files during periods of peak use. ■ Number of available threads for scanning This value defines the maximum number of scanning threads that Symantec Scan Engine generates. Symantec Scan Engine initializes 16 threads when the service starts. The value is incremented according to the load to a maximum of 128 threads. You can decrease the value based on your hardware configuration. The maximum value is 512 threads. See "Allocating resources for Symantec Scan Engine" on page 59.

Table 6-6 Configurations to enhance performance *(continued)*

Configuration	Description
Modify server resources	Symantec Scan 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 Scan 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 128 MB. The maximum value is 2048 MB (2 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 16 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 Scan Engine" on page 59.
Notify a file server when Symantec Scan 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 impact on performance, you can send the notification on demand, as needed. See "Notifying a file server when definitions are updated" on page 90.

Chapter 7

Filtering URLs

This chapter includes the following topics:

- About filtering URLs
- How to filter a URL

About filtering URLs

If your client uses ICAP, you can filter Web sites based on Uniform Resource Locator (URL) addresses. Symantec Scan 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 Scan Engine includes predefined URL categories that consist of URLs containing related subject matter. Symantec Scan Engine 5.2.11 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 Scan Engine notifies the ICAP client if a requested URL is listed in any URL category or local category. 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 Scan Engine operates in filtering mode, Symantec Scan Engine handles the application of URL filtering. You configure the types of URL that you want to deny. Based on your configuration, Symantec Scan Engine determines whether to deny access for each request. Symantec Scan Engine returns to the user an "Access Denied" message when it blocks access to a URL.

See "About the filtering modes" on page 148.

See "How to filter a URL" on page 148.

About categories

Symantec Scan Engine uses categories to determine whether access to a URL should be denied. Symantec Scan Engine provides predefined URL categories. You can also create additional categories (local categories) to meet your needs.

See "About local categories" on page 147.

About predefined URL categories

Table 7-1 provides information about the predefined URL categories that are included in Symantec Scan Engine.

Table 7-1 Predefined URL categories

URL Category	Description
Abortion	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.
Advertising	Sites that provide Internet advertising services such as Sponsored ads, search engine marketing, pop-up, banner ads and so on.
Alcohol	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.
Anonymizer	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.

Table 7-1 Predefined URL categories *(continued)*

URL Category	Description
Art and Museums	Sites that include art galleries, artists, and museums such as performing arts, theater, painting, drawing, sculpture, and photography are included.
Art Nudes	Sites that contain the non-pornographic, tasteful, and artful display of the naked body. The main purpose of these sites is not sexual arousal.
Automated Web Application	Sites that allow a computer to automatically open an HTTP connection for reasons such as checking for operating system or application updates.
Automotive	Sites that relate to manufacturers of motor vehicles, automotive dealers, motor sports, and clubs.
Bikini	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.
Blog	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.
Business	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.
CAIC	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.
Cash Gambling	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.
Chat	Sites that enable online chatting in real time. These can include text-based chat, Instant Messaging chat, and visual chat rooms.

Table 7-1 Predefined URL categories *(continued)*

URL Category	Description
Criminal Skills	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.
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. ■ Ontario Consultants on Religious Tolerance, http://www.religioustolerance.com/ - Scholarly collection of researched topics and elaborate categorization of all belief systems.
Drugs	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.

Table 7-1 Predefined URL categories *(continued)*

URL Category	Description
Dynamic	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.
Education	Sites that represent schools or other educational facilities, faculty, or alumni groups such as homeschooling, public and private schools, universities and colleges.
Energy	Sites that represent companies involved with the production and distribution of energy such as oil companies, gas companies, power companies, and alternative energy companies.
Enterprise Webmail	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.
Entertainment	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.
File sharing	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.
Finance and Investing	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.
Food and Restaurants	Sites that provide information, guides, and reviews about restaurants; specialty food shops, food recipes, and food delivery.
Forums and Message Boards	Sites that provide message boards and forums where users can discuss numerous topics. Sites that provide monitored or unmonitored Web forums, Bulletin boards, etc.
Freeware and Shareware	Sites that make software available for downloading to users such as freeware, shareware, or open source software.
Gambling	Sites that provide online casinos, lotteries, information and instructions about placing bets, allowing to bet online and participate in betting pools, and online Gambling.
Gaming	Sites that are dedicated to online games, game tips, game downloads, interactive games, and multiplayer games.

Table 7-1 Predefined URL categories *(continued)*

URL Category	Description
Glamour	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.
Gore	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.
Government	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.
Hacking	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.
Hate	Sites that promote hostility against particular individual or group on the basis of race, religion, color, gender, and origin.
Health	Sites that provide information about personal health and medical services, hygiene, diets, therapies, and counseling services about health.
Hobbies	Sites that provide information about personal interests like collectibles, crafts, pets, and past times.
Hosting	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.
Internet Telephony	Sites that provide the facility for telephone calls by Internet, or provide information or software for the purpose.
Job Search	Sites that are dedicated to job searches, job listings, creating and posting resumes, and organizing job fairs.
Kids	Sites that are dedicated to children activities such as artwork, school projects, crafts, information to answer their questions, and games.

Table 7-1 Predefined URL categories *(continued)*

URL Category	Description
Law	Sites that contain legal information about state and regional laws, lawyers, legal services, legal consultations.
Lifestyle	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: ■ Sites dedicated to GLBT orientation issues, resources, outreach, portals, clubs, associations, personal sites (personal home pages), and activism. ■ 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. ■ Family, adoption, or marriage or partner concerns and rights within target groups ■ 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 conisered as GLBT issues. ■ 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. ■ 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.

Table 7-1 Predefined URL categories *(continued)*

URL Category	Description
Mature Content	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. ■ Sexual relationship counseling ■ Products to improve one's sex life ■ Explicit discussions of sex and sexuality ■ Sexual orientation issues ■ Lingerie sales ■ Nudism or Naturism ■ 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.
Military	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.
Mobile Entertainment	Sites that offer a range of add-ons for handheld devices like ringtones, wallpapers, games, and videos.
Music	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.
News	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: ■ Mainstream news services, daily news, local or regional news ■ Alternative news ■ Internet news broadcasts (audio or video) ■ News-oriented online and print magazines or newspapers ■ News services or personalized news ■ Editorials or opinion columns
Non profit	Sites that are owned by non-profit organizations. A non-profit organization (abbreviated "NPO", also "not-for-profit") 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.

Table 7-1 Predefined URL categories *(continued)*

URL Category	Description
Occult	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: ■ Magic spells and curses, encompassing both self-defined "black" and "white" magic ■ Chaos Magick, Crowley, Golden Dawn, Ordo Templi Orientalis ■ Demonolatry (worship of demons) ■ Witchcraft and its practices, rituals, and activities, Wiccan magic, Pagan/neo-Pagan magic. Asatru (Odinism) ■ Vodun (Voodoo/Santeria) ■ Herbs, tools or paraphernalia for casting spells, summoning demons, or engaging in other magical behavior or activities
Personal Ads and Dating	Sites that promote or provide opportunity for establishing or continuing romantic or sexual relationships. Examples are: ■ Dating portals and directories ■ Personal ads like general, regional, lifestyle, 900 numbers, personal pages that promote or provide personal ads ■ Cyber relationships ■ Dating portals ■ Directories ■ Cyber relationships and dating services, matchmaking services, and e-dating services ■ International introductions, pen pal agencies, and introduction agencies
Pets	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: ■ Pet care ■ Pet products ■ Animal rescue ■ Pet breeding

Table 7-1 Predefined URL categories *(continued)*

URL Category	Description
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.

Table 7-1 Predefined URL categories *(continued)*

URL Category	Description
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
Reference	Sites that contain personal, professional, or educational references. Examples are: ■ Online dictionaries, encyclopedias, thesauri ■ Maps and language translation sites
Religion	Sites on religion as any set of beliefs and practices that have the function of addressing the fundamental questions of human identity, ethics, death, and the existence of the Divine.
Science	Sites that provide research materials in the natural and life sciences.
Search	Sites that support searching the Internet, newsgroups , or indices and directories.

Table 7-1 Predefined URL categories *(continued)*

URL Category	Description
Self Harm	Sites that describe or discuss ways in which to self harm including eating disorders and self-injury. Eating disorders sites include: ■ Sites about Anorexia, Bulimia, and Binge eating disorder or compulsive overeating, compulsive over-exercising, pica, prader-willi syndrome, night eating syndrome, body dysmorphic disorder, othorexia, and bigorexia ■ Sites supporting eating disorder as a lifestyle choice covering issues like diet and exercise methods, how to hide your eating disorder, the thin commandments, and so on. ■ Personal pages, journals, blogs, forums, webrings supporting an eating disorder lifestyle ■ Picture pages or galleries created for inspiring people with eating disorders, for example, thinspiration, thinspo. Self-injury sites include: ■ Sites about self-injury including cutting, punching, hitting, scratching, choking, self-biting, picking at wounds, and self-poisoning. ■ Personal pages, forums, and clubs that may trigger self-injurious behavior ■ Self injury webrings ■ Pictures of self injury
Sexual Education	Sites that provide educational information on reproduction and sexual development, sexually transmitted disease, contraception, safe sexual practices, sexuality, and sexual orientation.
Shopping	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: ■ 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

Table 7-1 Predefined URL categories *(continued)*

URL Category	Description
Sports	Sites that promote or provide information about spectator sports. Examples are: ■ 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
Technology and Telecommunications	Sites that provide information pertaining to computers, the Internet as well as telecommunication. Examples are: ■ Software solutions and services ■ Computer and telecommunication hardware, devices, and gadgets ■ Internet and phone access services ■ Technology news

Table 7-1 Predefined URL categories *(continued)*

URL Category	Description
Tobacco	Sites that encourage, promote, offer for sale or otherwise encourage the consumption of tobacco. Examples are: ■ Retailers and manufacturers from the tobacco industry ■ Tobacco products and paraphernalia ■ Smoking is good, glamorous, or cool ■ How to smoke or smoking lessons
Travel	Sites that promote or provide opportunity for travel planning in a general sense, particularly finding, and making travel reservations. Examples are: ■ Travel portals, packages, and information (includes tours, travel clubs and associations, and travel information for specific demographic groups) ■ Air travel (air carriers: tickets/reservations/charters) ■ Sites that facilitate travel-related transportation (tickets/reservations/charters/rentals of trains, buses, boats, motorcycles. Does not include car rentals.) ■ Lodging (includes lodging directories and portals) ■ Travel agents and travel auctions
Violence	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: ■ Explosives and bombs: How to manufacture, obtain materials, transport, or seed an area, including but not limited to making explosives using common household items. ■ Pranks, destructive mischief, "revenge," teenage anarchy including but not limited to dangerous chemistry ■ Descriptions or instructions for killing people
Virtual Community	Sites that offer a variety of tools and mechanisms to enable a group of people to communicate and interact by the Internet. Examples include: ■ Social networking ■ Chat and instant messaging ■ Forums & Messageboards ■ Hosting of home pages and other user generated content including audio and video

Table 7-1 Predefined URL categories *(continued)*

URL Category	Description
Weapons	Sites that describe or offer for sale weapons including guns, ammunition, firearm accessories, knives, and martial arts. Examples are: ■ Online sales of firearms, ammunition, accessories, and knives ■ Descriptions, reviews, specifications, or weapons ■ Weapons retailers, manufacturers, auctions, and trading centers ■ Instructions for manufacture of weapons
Webmail	Sites that provide Web-based email services that are freely available and accessible through any Internet browser.
Wedding	Sites related to the traditions, customs, planning, and products involved in a marriage or commitment ceremony as well as in civil unions. Examples are: ■ Wedding planning ■ Wedding products ■ Alternative commitment ceremonies

Symantec periodically updates the predefined URL categories. If you subscribe to category updates, Symantec Scan Engine automatically downloads updated categories through LiveUpdate. Symantec might create new URL categories to address additional content areas as needed. If you subscribe to the category updates, any new categories are automatically downloaded with the regular updates to the existing categories. 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 viewed or modified.

See "Overriding a URL categorization" on page 154.

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.

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 151.

How to filter a URL

If your client uses ICAP, you can take advantage of the URL filtering capabilities of Symantec Scan Engine. You must have the appropriate URL filtering licenses to use the URL filtering features in Symantec Scan Engine.

See "About licensing" on page 69.

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" on page 149.
  See "About the filtering modes" on page 148.
- Specify the URLs (by subject content) to which you want to deny access.
  See "Denying access to URLs in URL categories" on page 150.
- Create and populate local categories with sites to which you want to deny user access.
  See "Managing local categories" on page 151.
- Override URL categorizations by adding URLs to Allow categories.
  See "Overriding a URL categorization" on page 154.
- Customize the "Access Denied" message that users see when access to a URL is denied.
  See "Customizing the access denied message" on page 155.

About the filtering modes

Symantec Scan Engine lets you scan URLs in audit mode or filtering mode. The mode that you use depends on the capabilities of the client application for which Symantec Scan Engine provides URL scanning. It also depends on the manner in which Symantec Scan Engine is deployed.

Note: When you change from audit mode to filtering mode, the URL category and local category settings revert to settings that you configured (and applied) in filtering mode.

About filtering mode

When Symantec Scan Engine operates in the filtering mode, Symantec Scan Engine handles URL filtering and the denial-of-access to restricted sites.

Specify the categories to deny. Based on your configuration, Symantec Scan Engine determines whether to deny access for each request. If access is denied, Symantec Scan Engine returns an "Access Denied" message to the user.

See "Customizing the access denied message" on page 155.

When Symantec Scan Engine scans in filtering mode, it stops scanning when the first URL match is found.

About audit mode

When Symantec Scan Engine operates in audit mode, the ICAP client handles the application of URL filtering and the denial-of-access to restricted sites.

Symantec Scan 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 151.

For each request from the ICAP client, Symantec Scan Engine matches the request against all categories. Symantec Scan Engine notifies the client if the requested URL is contained in any URL category or local category. Based on the information that Symantec Scan Engine returns, the ICAP client determines whether the site should be blocked.

When Symantec Scan Engine scans in audit mode, scanning does not stop when a single URL match is found. It continues to scan against all categories. Symantec Scan 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

Symantec Scan Engine is provided with minimum URL definitions. We recommend you to run LiveUpdate and update the URL definitions before you start URL scanning.

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

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 definitions**.

4 Under Enable URL filtering and download URL 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 Scan 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 "Overriding a URL categorization" on page 154.

Note: Symantec Scan 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 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 Scan Engine looks for the most exact match when checking a URL. 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 7-2 Filtering by URL

Filtered URL	Effect
www.symantecexample.com/pics/apr.html	Matches this one specific page
www.symantecexample.com/pics	Matches the entire directory
www.symantecexample.com	Matches this computer
symantecexample.com	Matches the entire domain

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 Scan 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 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 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 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 511 characters per URL) box, type the URL that you want to add.

   Type one URL per line. You can enter maximum 511 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 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 511 characters per URL) box.
3. In the URLs associated with selected Local Category (maximum 511 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.

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 Scan 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 definitions**.
4. Under URL List Override (maximum 511 characters per URL), type the URL for which you want to allow access.

   Type one URL per line. You can enter maximum 511 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.

Customizing the access denied message

Symantec Scan Engine displays an Access denied message to the user when access to a Web site is blocked. The default message is as follows:

The requested document, ${URL_REQUESTED}, will not be shown. ${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.

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 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.

Chapter 8

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 Symantec Scan Engine to log events to SSIM
- About configuring alerts
- About reports

About logging data

Symantec Scan 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 157.

See "Logging levels and events" on page 159.

Logging destinations

Table 8-1 shows the destinations to which Symantec Scan Engine can forward log events.

Table 8-1 Logging destinations

Destination	Description
Local logs	Symantec Scan Engine logs events to the local logs by default. The default location for the local logs for Solaris and Linux is /opt/SYMCScan/log. The default location for the local logs for Windows is 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 163.
Windows Application Event Log	If you are running Symantec Scan Engine on Windows, you can log events to the Windows Application Event Log. See "Configuring logging to the Windows Application Event Log" on page 168.
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" on page 167.
Symantec Security Information Manager	You can log events to the Symantec Security Information Manager for event management and correlation. Symantec Security Information Manager integrates multiple Symantec Enterprise Security products and third-party products to provide a central point of control for security within an organization. For more information about how to integrate Symantec Scan Engine with Symantec Security Information Manager, on the Internet, go to the following URL: https://www-secure.symantec.com/platinum/en/Collectors/ See "Configuring Symantec Scan Engine to log events to SSIM" on page 169.
RPC client logging subsystem (RPC only)	If your client uses RPC, Symantec Scan 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 91.

Table 8-1 Logging destinations *(continued)*

Destination	Description
Abort log	Information is logged to the abort log only when Symantec Scan Engine fails to start before the standard scan 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, ScanEngineAbortLog.txt. This file is located in the installation directory.
Microsoft Operations Manager 2005 (MOM)	You can integrate Symantec Scan Engine events with Microsoft Operations Manager 2005. Microsoft Operations Manager is a central repository you use to monitor critical events, errors, warnings, and information about your Symantec Scan Engine servers. Preconfigured Rule Groups and Child Rule Groups are automatically created when you import the management pack. These rules monitor specific Symantec Scan Engine events in the Windows Event Log. When a rule is triggered, the Microsoft Operations Manager agent collects data about the event and forwards it to the Microsoft Operations Manager. For more information, see the *Symantec™ Scan Engine Management Pack Integration Guide* on the Symantec Scan Engine product CD in the following location: Tools/ MOM_Management_Pack/ Docs/ SSE_Management_Pack_Integration_Guide.pdf

Logging levels and events

You can select a different logging level for each logging and alert notification destination. For example, Symantec Scan Engine can log Error logging level events to the local log. It can log Warning logging level events to the Windows Application Event Log. For each logging level, you can also choose the events for which messages are generated.

Table 8-2 lists the events for which messages are generated at each logging level.

Table 8-2 Events by logging level

Logging level	Events logged
None	None

Table 8-2 Events by logging level *(continued)*

Logging level	Events logged
Error	The following events are logged: ■ Definitions corrupted ■ Definitions update failure ■ Licensing error ■ Filer (RPC) retry error ■ Scan error ■ Critical error ■ Crash error ■ 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
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 ■ Infection outbreak alert ■ Virus outbreak alert ■ Container limit outbreak alert

Table 8-2 Events by logging level *(continued)*

Logging level	Events logged
Warning	The following events are logged: ■ All of the events that are logged at the Error logging level ■ Definitions rollback failed ■ Infection found ■ Spyware Risk ■ Adware Risk ■ Other Security Risk ■ Container violation found ■ File attribute violation found ■ Definitions rollback ■ Mail policy violation found ■ Licensing warning ■ URL block ■ File Access Allowed ■ Symantec Scan Engine has not received configured number of requests ■ Scanning feature hung or scan engine is overloaded ■ Scan request rejected ■ Failed to set Rapid Release parameters ■ Failed to create self scan test file
Information	The following events are logged: ■ All of the events that are logged at the Error logging level ■ Version information ■ URL audit detection ■ Definitions update ■ LiveUpdate up-to-date ■ LiveUpdate succeeded

Table 8-2 Events by logging level *(continued)*

Logging level	Events logged
Verbose	The following events are logged: ■ All of the events that are logged at the Error 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 is not available for SMTP alerts and SNMP alerts or SSIM logging. **Note:** The Verbose logging level should only be selected for debugging purposes. Performance is significantly degraded if you active this logging level for general logging.

Specifying the log bind address

You can set a log bind address for each Symantec Scan Engine so that you can more easily identify the originating scan engine. When you use this feature, the log bind address of the originating Symantec Scan Engine is included in all alert messages.

For example, setting the log bind address is helpful if you have multiple Symantec Scan Engines that listen on the loopback interface (127.0.0.1). The IP address on which Symantec Scan Engine listens is used in SNMP and SMTP alert messages to identify the originating Symantec Scan Engine. Therefore, it is not possible to determine which Symantec Scan Engine originated the message when more than one uses the loopback interface. You can set a unique log bind address for each Symantec Scan Engine to provide a method for identifying each Symantec Scan Engine.

If your client uses ICAP and you do not specify a log bind address, Symantec Scan Engine selects one for you. Symantec Scan Engine determines the log bind address based on the scanning bind addresses that you enable on the Configuration > Protocol page.

Symantec Scan Engine determines the log bind address based on the following conditions:

No bind address is selected in the ICAP Configuration Bind address table.	The logging bind address is the first bind address in the ICAP Configuration Bind address table on the Configuration > Protocol page. If the first bind address is the local host, then the Logging IP address is the second bind address in the list.
One or more bind addresses are selected in the ICAP Configuration Bind address table.	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 > Protocol page.

See "Configuring ICAP options" on page 80.

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 Scan 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 164.
- Change the directory where log files are located.
  See "Changing the directory where log files are located" on page 164.

See "Maintaining log files on a shared resource" on page 165.

- Change the length of time that the log files are maintained.
  See "Changing the length of time that log files are maintained" on page 166.
- Enable statistics reporting.
  See "Enabling statistics reporting" on page 167.

Specifying the local logging level

Symantec Scan 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.

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.

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 Solaris and Linux is opt/SYMC Scan/log. The default location for Windows is C:\Program Files\Symantec\Scan Engine\log\.

Symantec Scan 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.

See "Changing the length of time that log files are maintained" on page 166.

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 Scan 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

You can store the Symantec Scan 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 Scan Engine is installed.

Note: To enhance Symantec Scan 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 Scan Engine is installed. Also ensure that you have full permissions on the shared resource.

To maintain log files on a shared storage

1. Map or mount the shared resource from the host on which Symantec Scan 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 Scan Engine service.

   See "Verifying, stopping, and restarting the Symantec Scan Engine service on Windows" on page 47.

   See "Verifying, stopping, and restarting the Symantec Scan Engine daemon on Linux and Solaris" on page 46.

3. Change the account of the Symantec Scan Engine service to the Administrator.
4. Restart the Symantec Scan 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\scanengine\

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.

Changing the length of time that log files are maintained

Symantec Scan Engine creates a new log file for each day. You can specify the number of log files that Symantec Scan 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 1. That means that only the latest log file will be retained.

If needed, you can periodically export the data to another file to retain the log data before it is removed.

See "Exporting local log data to a file" on page 176.

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 (1) so that only the latest log file is 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

You can configure Symantec Scan 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 176.

The following information is logged to the statistics logs:

Infections	URL Audits
Repaired Infections	Total Files Scanned
Risks Detected	Files Scanned
Files Quarantined	URLs Scanned
Mail Policy Violations	Megabytes Scanned
Container Policy Violations	Requests
File Attribute Policy Violations	Connections to Scan Engine
Malformed Containers	Cumulative Scan Time (milliseconds)

URL Blocks Scan Errors

Symantec Scan 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 Solaris and Linux is /opt/SYMCScan/log.The default location for Windows is C:\Program Files\Symantec\ScanEngine\log\.

See "Changing the length of time that log files are maintained" on page 166.

To enable statistics reporting

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 statistics reporting**.

   Statistics reporting is enabled 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.

Configuring logging to the Windows Application Event Log

If you are running Symantec Scan Engine on Windows, you can configure Symantec Scan 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 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.

See "Logging levels and events" on page 159.

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.

Configuring Symantec Scan Engine to log events to SSIM

You must configure Symantec Scan Engine to communicate with SSIM by specifying the IP address and port number on which SSIM listens. You also can change the types of events that are logged to SSIM.

To configure Symantec Scan Engine to log events to SSIM

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 Symantec Security Information Manager, in the SSIM logging level drop-down list, select the appropriate logging level.

Logging to SSIM is not activated by default.

See "Logging levels and events" on page 159.

4 In the SSIM agent address box, type the IP address on which the local SSIM Agent listens.

The default setting is 127.0.0.1 (the loopback interface), which restricts connections to the same computer.

5 In the Port number box, type the TCP/IP port number on which the local SSIM Agent listens.

The port number that you enter here must match the port number on which the local SSIM Agent listens. The default port is 8086.

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.

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 170.

See "Activating SNMP alerts" on page 171.

If you activate SNMP or SMTP alerts and are running multiple Symantec Scan Engines, set a log bind address for each one. Separate log bind addresses let you identify the originating Symantec Scan Engine for each SNMP and SMTP alert message.

See "Specifying the log bind address" on page 162.

You also can activate outbreak alerts. Symantec ScanEngine 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 173.

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 Scan 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 "Logging levels and events" on page 159.

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 Scan Engine.

   The domain name is added to the From box for SMTP messages. SMTP alert messages that Symantec Scan Engine generates originate from SymantecScanEngine@<domainname> ,where <domainname> is the domain name that you specify in the SMTP domain box.
7. In the Email recipients box, type the email addresses of the recipients of the SMTP alert messages.

   Type one email address per line.
8. 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.

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 (symcscan.mib) is located in the MIB directory on the Symantec Scan Engine CD. You can use this file to configure SNMP alerts.

You must select the types of events for which SNMP alert messages are generated.

See "Logging levels and events" on page 159.

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.

Configuring outbreak alerts

Symantec Scan 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 Scan Engine generates an alert.

Table 8-3 lists the outbreak alert events that you can configure.

Table 8-3 Outbreak alert events

Event	Description
Any virus infections	A threat was detected **Note:** Outbreak alerts for security risks is not supported.
Same virus infections	One or more incidence of the same type of threat was detected
Mail policy violations	A mail policy violation occurred
Blocked URLs	A URL was blocked due to a URL filtering violation
Max extract	A maximum file extraction limit was met or exceeded
Malformed containers	A malformed container was detected and blocked
File attribute	Any file attribute violation was detected

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.

   See "Logging levels and events" on page 159.

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.

About reports

You can use the Symantec Scan 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.

You can manage reports through the Symantec Scan 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 175.
- Export selected local log data in a comma-separated value (.csv) format.
  See "Exporting local log data to a file" on page 176.
- 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 176.

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 159.

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**.

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 Scan 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**.

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
- Total megabytes scanned
- Types of violations that Symantec Scan Engine found by violation type

---

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.

See "Enabling statistics reporting" on page 167.

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 Scan Engine is the local logs. The default location for the local logs on Solaris and Linux is /opt/SYMCScan/log. The default location for Windows 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 164.

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**.

Chapter 9

Keeping your product and protection up-to-date

This chapter includes the following topics:

- About content updates
- About LiveUpdate
- About Intelligent Updater
- About Rapid Release
- Rolling back definitions

About content updates

You can update the Symantec Scan Engine content. The content updates ensure that your Symantec Scan Engine server is up-to-date with the most current antivirus and URL definitions. You can update Symantec Scan Engine with the latest definitions without any interruption in scanning.

See "About licensing" on page 69.

About definition updates

Symantec provides updates for the following types of definitions:

Security risks	Definition files contain the necessary information to detect and eliminate risks, such as viruses and adware. Symantec supplies updated definition files at least every week and whenever a new risk is discovered. You can update risk definitions using LiveUpdate, Rapid Release, or Intelligent Updater.
URL	Symantec periodically supplies updated URL definition files. If you subscribe to content updates, Symantec Scan 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.

Symantec Scan Engine automatically uses the most current definitions 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 Scan Engine downloads and installs the most current definitions. If an error occurs, Symantec Scan Engine tries to roll back to the previous definitions. If the rollback is successful, Symantec Scan 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 192.

See "About licensing" on page 69.

About updating your protection

You can use several methods to update protection from risks and HTTP content filtering violations with Symantec Scan Engine.

Table 9-1 lists the methods that you can use to obtain updated definitions from Symantec.

Table 9-1 Methods to obtain updated definitions from Symantec

Method	Description	How often Symantec provides updated definitions
LiveUpdate	Use LiveUpdate to automatically update your protection. When LiveUpdate runs, it only downloads and installs definitions that are more current than the definitions that are found on the Symantec Scan Engine server. You can configure LiveUpdate to run on a scheduled basis, or you can run it manually. See "About LiveUpdate" on page 182.	Weekly, except in cases of outbreaks, when definitions are updated more often
Rapid Release	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 190.	Hourly
Intelligent Updater	Use Intelligent Updater if your organization has a high-speed Internet connection and is at a high risk of exposure to threats and security risks. You download Intelligent Updater definitions from the Symantec Web site. **Note:** Intelligent Updater does not provide updated URL definitions. See "About Intelligent Updater" on page 187.	Daily

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 69.

About LiveUpdate

When you install or upgrade Symantec Scan 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 Scan Engine tries to perform a LiveUpdate.

See "Configuring the number of LiveUpdate retries" on page 229.

See "Configuring LiveUpdate to occur automatically" on page 182.

See "Performing LiveUpdate on demand" on page 183.

When Symantec Scan 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.

See "Rolling back definitions" on page 192.

Symantec Scan Engine uses Symantec Java LiveUpdate technology. To run LiveUpdate, you must have the Java 2SE Runtime Environment (JRE) 5.0 (update 13 or later) or JRE 6.0 installed.

Configuring LiveUpdate to occur automatically

You can schedule LiveUpdate to occur automatically at a specified time interval to ensure that Symantec Scan Engine always has the most current definitions. When you install a valid antivirus content license or URL content license, Symantec Scan Engine automatically tries to perform a LiveUpdate. By default, Symantec Scan 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 Scan 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 "Changing the LiveUpdate base time" on page 229.

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.
4. 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.
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.

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 Tasks, click **LiveUpdate Content**.

About scheduling LiveUpdate using the command-line

You can use the command-line to schedule LiveUpdate. LiveUpdate ensures that Symantec Scan Engine always has the most current definitions. On Solaris and Linux, definition updates can be scheduled using the UNIX cron scheduler. You must create an empty file within the directory in which Symantec Scan Engine is installed. The empty file name must be LUNowFlag. Symantec Scan Engine periodically checks for this file and performs a LiveUpdate when this file is present. Symantec Scan Engine automatically removes the file before the LiveUpdate command runs.

If you are using Windows, you can schedule definition updates using a schedule utility. The utility creates a LUNowFlag file in the Symantec Scan Engine installation directory.

About setting up your own LiveUpdate server

If you have multiple Symantec Scan 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 Scan Engine on your network contact Symantec servers.

For more information, see the *LiveUpdate Administration Utility*, which is included on the Symantec Scan Engine CD.

See "Where to get more information" on page 26.

If you set up your own LiveUpdate server, you must edit the LiveUpdate configuration for Symantec Scan Engine to point to the local LiveUpdate server. The Symantec Scan Engine LiveUpdate configuration file contains the configuration options for LiveUpdate. For Solaris and Linux , the default location is /opt/SYMCScan/bin/. For 32-bit Windows, the default location is C:\Program Files\Symantec\Scan Engine and C:\Program Files(x86)\Symantec\Scan Engine for 64-bit Windows

About editing the LiveUpdate configuration file

You must configure LiveUpdate in the configuration file so that Symantec Scan Engine always has the most current definition files.

See "Editing the Symantec Scan Engine configuration files" on page 219.

From Symantec Scan Engine 5.2.10, some new parameters have been added to the liveupdate.conf file.

Table 9-2lists the new parameters that are added to the liveupdate.conf file.

Table 9-2 New Parameters in liveupdate.conf file

Parameter	Description
cacheMode	Disables caching of the definitions that are being downloaded. Initially the definitions are downloaded to the temporary working directory. If caching is disabled, the folders with the timestamp are deleted once the download is complete. For example, `cacheMode=false`
downloadCacheSize	The maximum size the Java LiveUpdate cache can grow until it is eligible for purging. If CacheMode is true, this parameter needs to be configured, otherwise, Java LiveUpdate fails. For example, `downloadCacheSize=5368709120`
maxPackageContentSize	The maximum allowed size of the package contents. For example, `maxPackageContentSize=2147483647`
maxPackageSize	The maximum allowed size of the package file. For example, `maxPackageSize=2147483647`

Selecting the transport protocol

Updated definition files are retrieved through HTTP or FTP. This information is required unless you use a host file. The default setting for the LiveUpdate transport protocol is HTTP.

To select the transport protocol

- In the configuration file at protocol=, type **FTP** or **HTTP** as appropriate.

Selecting the LiveUpdate host

Symantec Scan Engine contacts a specified host to check for and to retrieve updated definition files. You must supply the appropriate LiveUpdate host name. A LiveUpdate host is required unless you use a host file. The default host is liveupdate.symantec.com.

To select the LiveUpdate host

- In the configuration file at host=, type the new host name.

Specifying the directory on the LiveUpdate host (FTP only)

If you retrieve updates through FTP, you must specify the directory on the LiveUpdate host that contains the LiveUpdate packages. For example, on a UNIX system, the directory would be as follows:

/opt/Symantec/LiveUpdate/downloads

To specify the directory on the LiveUpdate host (FTP only)

- In the configuration file at packagedir=, type the appropriate directory path.

Specifying the logon name (FTP only)

If you retrieve updates through FTP, you must specify a user name and password to log on to the FTP site.

To specify the logon name (FTP only)

- In the configuration file at logon=, type the user name.

Specifying a password (FTP only)

If you retrieve updates through FTP, you must specify a password to log on to the FTP site.

To specify a password (FTP only)

- In the configuration file at password=, type the password.

Specifying a temporary working directory

LiveUpdate requires the use of a working temporary directory on the computer on which Symantec Scan Engine is running. You must supply a temporary directory location.

To specify a temporary working directory

- In the configuration file at workdir=, type the path for the temporary directory.

Specifying a log file path

You can specify where you want to store the LiveUpdate activity log file.

Specifying a log file path

- In the configuration file at logfile=, type the log file path where you want to store the LiveUpdate activity log file.

  The following is an example of a log file path for Windows:

  logfile=C:\WINNT\Temp\LiveUpdate.log

Allowing downloads from URLs

You can permit downloads from the URLs that are specified in the .TRI entry.

To allow downloads from URLs

- In the configuration file at urls=, type **1** to allow downloads from the specified URL, or type **0** to prevent downloads.

Specifying a proxy server

If you retrieve updates through HTTP and your network requires Internet requests to proxy through another server, specify those proxy settings in the LiveUpdate configuration file.

To specify a proxy server

- In the configuration file at proxy=, type the proxy server host name or IP address and the port number (separated by a colon).

  You must use the following format:

  <servername>:<portnumber>

  where <servername> is the IP address or host name of the proxy server, and <portnumber> is the appropriate port.

About Intelligent Updater

You can use Intelligent Updater if your organization has a high-speed Internet connection and has a high risk of exposure to threats or security risks. You download Intelligent Updater definitions from the Symantec Web site.

Note: Intelligent Updater does not support updating URL definitions updates. You must update URL definitions using LiveUpdate.

See "About LiveUpdate" on page 182.

Symantec provides the latest definition files for download on the Symantec Web site through Intelligent Updater. Intelligent Updater is updated daily with the most current definition files.

The name of the Intelligent Updater file, which changes with each update, uses the following format:

```
yyyymmdd-vvv-Pbb.exe
```

The file name provides the following information:

```
yyyy     year
mm       month
dd       day
vvv      version
P        processor (I=Intel, A=Alpha)
bb       platform (16=16-bit, 32=32-bit)
```

For example, 20080225-003-i32.exe is the February 25, 2008 build version three, Intel 32-bit update for Windows.

Note: Intelligent Updater file downloads are larger than LiveUpdate file downloads and Rapid Release file downloads. The downloads are larger because LiveUpdate and Rapid Release add definitions to the current definitions set. Intelligent Updater replaces the current definition set with a new definitions set that contains both old and the new definitions.

Symantec Scan Engine must be running when you install definitions using Intelligent Updater to ensure that the newer definitions become the active definitions set.

Enabling definition updates through Intelligent Updater

By default, Symantec Scan Engine does not support updating definitions with Intelligent Updater. To enable Intelligent Updater, you must run a setup script for your platform.

To enable Intelligent Updater for Windows

1 At the command line, change directory to Symantec Scan Engine AntiVirus definitions directory. The directory is as follows:

```
<default directory>\Program
Files\Symantec\ScanEngine\Definitions\AntiVirus
```

2 Run the following script to enable the Intelligent Updater:

```
setup-iu.bat enable
```

A `shadow.iu` file is created in the present working directory. Symantec Scan Engine checks shared definitions once per minute.

Note: The Intelligent Updater does not work if the `shadow.iu` file is not present in the Symantec Scan Engine AntiVirus definitions directory.

To disable Intelligent Updater for Windows

1 At the command line, change directory to Symantec Scan Engine AntiVirus definitions directory. The directory is as follows:

```
<default directory>\Program
Files\Symantec\ScanEngine\Definitions\AntiVirus
```

2 Run the following script to disable the Intelligent Updater:

```
setup-iu.bat disable
```

Symantec Scan Engine performs updates through LiveUpdate.

To enable Intelligent Updater for Solaris or Linux

1 Change directory to Symantec Scan Engine AntiVirus definitions directory. The directory is as follows:

```
<default directory>/opt/SYMCScan/bin/definitions/AntiVirus
```

2 Run the following script to enable the Intelligent Updater:

```
setup-iu.sh enable
```

A `shadow.iu` file is created in the present working directory. Symantec Scan Engine checks shared definition once per minute.

Note: The Intelligent Updater does not work if the `shadow.iu` file is not present in the Symantec Scan Engine AntiVirus definitions directory.

To disable Intelligent Updater for Solaris or Linux

1. Change directory to Symantec Scan Engine AntiVirus definitions directory. The directory is as follows:

   ```
   <default directory>/opt/SYMCScan/bin/definitions/AntiVirus
   ```

2. Run the following script to disable the Intelligent Updater:

   ```
   setup-iu.sh disable
   ```

   Symantec Scan Engine performs updates through LiveUpdate.

About Rapid Release

You can configure Symantec Scan Engine to obtain uncertified definition updates with Rapid Release. You can configure Symantec Scan Engine to retrieve Rapid Release definitions every 5 minutes to every 120 minutes.

See "Configuring Rapid Release updates to occur automatically" on page 191.

See "Performing Rapid Release updates on demand" on page 192.

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 Updater 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.

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 192.

Rapid Release does not support URL definition updates. You must update URL definitions using LiveUpdate.

See "About LiveUpdate" on page 182.

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 Scan 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.

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 Scan 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.

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**.

Rolling back definitions

Symantec Scan 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 (roll back) to the previous set of antivirus or URL definitions. You can roll back definitions regardless of the method that is used to obtain the definitions. For antivirus and URL definitions sets, from Symantec Scan Engine 5.2.10 onwards, you can perform only one rollback.

Symantec Scan Engine installs with the most current definitions that are available at the time the product is released. After you install the product and active 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 69.

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 roll back 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 roll back.

   To select multiple definitions, press and hold the **CTRL** key and select the definitions that you want to roll back.
4. In the sidebar under Tasks, click **Rollback <definition feature name> Definitions**.

Appendix A

Performing a silent installation

This appendix includes the following topics:

- About silent installation and upgrade
- Implementing a silent installation in Solaris and 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 Scan Engine. You can use the silent installation feature when you install or upgrade multiple Symantec Scan Engines that have identical input values.

In Solaris and 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.

Implementing a silent installation in Solaris and Linux

Implementing a silent installation in Solaris and Linux involves the following process:

- Create a response file to capture your input values for installation.
- Run the installation program to read the response file.
  This response file lets you perform the installation silently using the values that you specified.

Creating the response file

To implement a silent installation in Solaris and 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 Scan Engine.

A default response file, called response, is included on the Symantec Scan Engine CD. The response file is a text file that is preconfigured with the default settings for the Symantec Scan Engine installation options. You must edit this response file so that it contains the input values that you want for the silent installation.

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 A-1 Input values in the response file

Input name	Description
Upgrade	Specifies that the installation is an upgrade. Possible values are as follows: ■ NONE Use this value if you do not want to perform an upgrade. This value is the default value. ■ UPGRADE 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. ■ CLEAN Use this value to uninstall and reinstall the product. Configure the input values that you want to modify.

Table A-1 Input values in the response file *(continued)*

Input name	Description
AdminPort	The port number on which the Web-based console listens. The default port number is 8004.
AdminPassword	The encrypted password for the virtual administrative account that you use to manage Symantec Scan Engine. If you do not specify a password, the default is blank (no password). **Note:** You must use the XML modifier command-line tool to generate an encrypted password. This tool is included on the product CD. Use the encrypted string that the tool returns for this value. See "Generating an encrypted password" on page 200.
SSLPort	The Secure Socket Layer (SSL) port number on which encrypted files are transmitted for increased security. The default port number is 8005.
InstallDir	The location where to install Symantec Scan Engine. The default location is /opt/SYMCScan.
User	The name of an existing user under which Symantec Scan Engine runs. The default setting is root.
JavaCmd	The full path (can be a symlink) to the Java 2SE Runtime Environment (JRE) 5.0 (update 13 or later) and JRE 6.0 executables.
JavaBinDir	The full path (can be a symlink) to the Java 2SE Runtime Environment (JRE) 5.0 (update 13 or later) and JRE 6.0 directory. The installer assumes that the path that you enter is correct. If the path is incorrect or the JRE version is not the correct version, Symantec Scan Engine does not function properly. (Symantec Scan Engine might not function properly even if the installer reports that the installation was successful.)

Table A-1 Input values in the response file *(continued)*

Input name	Description
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: .../lib/<architecture>/client 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/i386. Use the shorter path. If you have installed the JDK, use <JDK Dir>/jre/lib/i386. If you have installed the JRE, use <JRE Dir>/lib/i386. For Solaris, the path you enter should point to .../lib/sparc/client. If you have installed the JDK, use <JDK Dir>/jre/lib/sparc/client. If you have installed the JRE, use <JRE Dir>/lib/sparc/client. The installer assumes that the path that you enter is correct. If the path that you provide is incorrect, Symantec Scan 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.
EnableFilteringAnd DownloadDefinitions	Enables URL Scanning and downloading of the URL definitions. Possible values are as follows: ■ true: Use this value if you want to enable URL scanning in filtering mode and Download URL definitions. ■ false: Use this value if you want to disable URL Scanning and Definition Download. This is the default value.

To create the response file for Solaris and Linux

1. Locate the response file, response, on the Symantec Scan Engine CD and copy it to the /tmp directory.

   For the silent installation to initiate, the response file must be located in the /tmp directory.

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 200.

5. Save the file.

About initiating a silent installation using the response file

Ensure that the appropriate response file, called no-ask-questions, is located in the /tmp directory. 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 /tmp directory tells the installer to perform a silent installation with the input values in the file.

Note: The no-ask-questions file is not deleted after a silent installation.

About implementing a silent installation for Windows

The 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 A-2 Input values on the command-line

Input name	Description
INSTALLDIR	The location to install Symantec Scan Engine. The default location is C:\Program Files\Symantec\Scan Engine for 32-bit Windows platform, and C:\Program Files (x86)\Symantec\Scan Engine for 64-bit Windows platform.
USERUPGRADESELECTION	Specifies that the installation is an upgrade. Possible values are as follows: ■ UPGRADE Use this value to preserve your existing settings. All other input values are ignored. ■ CLEAN Use this value to uninstall and reinstall the product. Configure the input values that you want to modify.
ADMIN_PORT	The port number on which the Web-based console listens. The default port number is 8004.
SSL_PORT	The Secure Socket Layer (SSL) port number on which encrypted files are transmitted for increased security. The default port number is 8005.
ENCRYPTED_PASSWORD	The encrypted password for the virtual administrative account that you use to manage Symantec Scan Engine. If you do not specify a password, the default is blank (no password). **Note:** You must use the XML modifier command-line tool to generate an encrypted password. This tool is included on the product CD. Use the encrypted string for this value that the utility returns. See "Generating an encrypted password" on page 200.

Table A-2 Input values on the command-line *(continued)*

Input name	Description
ENABLE_URL_FILTERING	Enables URL Scanning and downloading of the URL definitions. Possible values are as follows: ■ true: Use this value if you want to enable URL scanning in filtering mode and Download URL definitions. ■ false: Use this value if you want to disable URL Scanning and Definition Download. This is the default value.
SSE_SERVICE _ACC_PWD	The password for the service account if the previous Symantec Scan 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 Scan 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.

Initiating a silent installation on Windows

Use the following procedures to initiate a silent installation on Windows.

To initiate a silent installation on Windows

1. Change directories to the location of the Symantec Scan 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=8006"
   ```

   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.

Generating an encrypted password

Use the XML modifier command-line tool to protect the administrative password that is used to manage Symantec Scan 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 CD.

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 Scan Engine console.

   The tool returns an encrypted string.
2. Save the entire encrypted string that the tool returns.

Appendix B

Using the Symantec Scan Engine command-line scanner

This appendix includes the following topics:

- About the Symantec Scan Engine command-line scanner
- Setting up a computer to submit files for scanning
- C-based command-line scanner syntax and usage
- Java-based command-line scanner syntax and usage

About the Symantec Scan Engine command-line scanner

The Symantec Scan Engine command-line scanner is a multi-platform utility that works with version 4.0.4 or later of Symantec Scan Engine. Symantec Scan Engine must be running on supported versions of Windows, Solaris, or Linux. The command-line scanner acts as a client to Symantec Scan Engine through the Symantec Scan Engine application programming interface (API). It uses version 1.0 of the Internet Content Adaptation Protocol (ICAP), presented in RFC 3507 (April 2003).

Symantec Scan 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 203.

- 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 213.

Use the command-line scanner to send files to Symantec Scan 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 Scan Engine operation.

Setting up a computer to submit files for scanning

You can send files to Symantec Scan Engine by using the command-line scanner. You can run this tool from the computer on which Symantec Scan 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 Scan Engine is installed.

To use the command-line scanner, you must select ICAP as the communication protocol for Symantec Scan Engine.

Because files are sent to Symantec Scan 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 Scan 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 Scan Engine.

You can use the command-line scanner to submit files for scanning from a computer that does not have Symantec Scan 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 Scan 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:
   - On the Symantec Scan Engine CD, in the top-level Command_Line_Scanner directory.
   - On the computer on which Symantec Scan Engine is installed, in the Symantec Scan Engine installation directory, in the ssecls subdirectory (Linux/Solaris) 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.

C-based command-line scanner syntax and usage

The C-based command-line scanner uses the following general syntax:

ssecls [-options] <path> [<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 Scan 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:

ssecls [-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 Scan Engine to descend into subdirectories to scan additional files, you must also use the -recurse option.

See "About requesting recursive scanning" on page 211.

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 Scan 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 Scan Engine.

Supported command-line options for C-based command-line scanner

Table B-1 describes the options that the command-line scanner supports.

Table B-1 Supported options for the C-based command-line scanner

Option	Description
-server	Specify one or more Symantec Scan Engines for scanning files. You must separate multiple entries with a semicolon. If you do not specify a Symantec Scan Engine, the server option defaults to the local host that listens on the default port. The format for each Symantec Scan Engine is <IPaddress:port>, where IPaddress is the DNS name or IP address of the computer on which Symantec Scan Engine is running, and port is the port number on which Symantec Scan Engine listens. **Note:** When more than one Symantec Scan Engine is specified, the load balancing and failover features of the API are activated automatically. See "About specifying the Symantec Scan Engine IP address and port for C-based command-line scanner" on page 206.

Table B-1 Supported options for the C-based command-line scanner *(continued)*

Option	Description
-mode	Optionally override the default antivirus scanning mode. The scanning modes that you can select are as follows: ■ scanrepairdelete If you do not specify a scanning mode, the scan policy defaults to scanrepairdelete. Symantec Scan Engine tries to repair infected files. Files that cannot be repaired are deleted. This configuration is the recommended setting. ■ scan Files are scanned, but no repair is tried. Infected files are not deleted. ■ scanrepair Symantec Scan Engine tries to repair infected files. Files that cannot be repaired are not deleted. See "About specifying the antivirus scanning mode for C-based command-line scanner" on page 207.
-verbose	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. See "About using the -verbose option" on page 208.
-details	Report detailed information about the infections or violations that are found. 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. **Note:** 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. See "About using the -details option" on page 209.

Table B-1 Supported options for the C-based command-line scanner *(continued)*

Option	Description
-timing	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 Scan Engine to scan the file. See "About using the -timing option" on page 210.
-recurse	Recursively descend into the subdirectories that are inside each path that is specified on the command-line. See "About requesting recursive scanning" on page 211.
-onerror	Specify the disposition of a file that has been modified (repaired) by Symantec Scan Engine when an error occurs when Symantec Scan 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 "About disposing of infected files when an error occurs" on page 211.

About specifying the Symantec Scan Engine IP address and port for C-based command-line scanner

The -server option lets you specify one or more Symantec Scan Engines for scanning files. If you do not specify a Symantec Scan Engine, the server defaults to the local host that listens on the default port.

The format for each Symantec Scan Engine entry is <IPaddress:port>, where IPaddress is the DNS name or IP address of the computer on which Symantec Scan Engine is running, and port is the port number on which Symantec Scan Engine listens. You only need to specify the port number if Symantec Scan 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 Scan 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 Scan Engine is specified, the load balancing and failover features of the API are activated automatically. The Symantec Scan Engine API provides scheduling across any number of computers that are running Symantec Scan Engine. When multiple Symantec Scan Engines are used, the API determines which Symantec Scan Engine should receive the next file based on the scheduling algorithm.

If a Symantec Scan Engine is unreachable or stops responding during a scan, another Symantec Scan Engine is called. The faulty Symantec Scan Engine is taken out of rotation for 30 seconds. If all of Symantec Scan Engines are out of rotation, the faulty Symantec Scan Engines are called again.

The API does not stop trying to contact Symantec Scan 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

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 Scan 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 Scan Engine tries to repair infected files. Files that cannot be repaired are not deleted.

For example:

ssecls -server 192.168.0.100:1344 -mode scanrepair c:\temp

When files are sent to Symantec Scan Engine using the command-line scanner, the command-line scanning mode overrides the scan policy configuration on Symantec Scan 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.

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 208.
- -details
  See "About using the -details option" on page 209.
- -timing
  See "About using the -timing option" on page 210.

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:

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 B-2 Possible scan result codes for the -verbose option

Result code	Description
-2	An error occurred within Symantec Scan Engine. The file was not scanned.
-1	An error occurred within the command-line scanner. The file was not scanned.

Table B-2 Possible scan result codes for the -verbose option *(continued)*

Result code	Description
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:

c:\work\filea -1

c:\work\fileb 2

c:\work\filec 2

c:\work\filed 0

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:

Problem name	Virus name or description of the container violation
Problem ID	Virus ID for viruses or pseudo-ID for policy violations
Disposition	Infected, repaired, or deleted

Note: The output data mirrors the information that Symantec Scan 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

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 Scan Engine to scan the file.

The reported scan time is calculated as the elapsed time between when the connection with Symantec Scan 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

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 Scan 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.

About disposing of infected files when an error occurs

The -onerror option specifies how to dispose of a file that Symantec Scan Engine 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 Scan 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 Scan 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

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 Scan 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.

Java-based command-line scanner syntax and usage

The Java-based command-line scanner 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 Scan 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-3 describes the options that the command-line scanner supports.

Table B-3 Supported options for the Java-based command-line scanner

Option	Description
-s, --server	Specify one or more Symantec Scan 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 Scan Engine, the server option defaults to the local host that listens on the default port. The format for each Symantec Scan Engine is <IPaddress:port>, where IPaddress is the DNS name or IP address of the computer on which Symantec Scan Engine is running, and port is the port number on which Symantec Scan Engine listens. **Note:** When more than one Symantec Scan Engine is specified, the load balancing and failover features of the API are activated automatically. See "About specifying the Symantec Scan Engine IP address and port for java-based command-line scanner" on page 215.
-a, --action	Optionally override the default antivirus scanning mode. The scanning modes that you can select are as follows: ■ scan Files are scanned, but no repair is tried. Infected files are not deleted. ■ scanrepair Symantec Scan Engine tries to repair infected files. Files that cannot be repaired are not deleted. ■ scanrepairdelete Symantec Scan Engine tries to repair infected files. Files that cannot be repaired are deleted. This configuration is the recommended setting. ■ Default If you do not specify a scanning mode, the scan policy defaults to policy set on the Symantec Scan Engine. See "About specifying the antivirus scanning mode for Java-based command-line scanner" on page 216.
-c, --clobber	Always overwrites the scanned file with server response.
-b, --verbose	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. See "About using the --verbose option in the java-based command-line scanner" on page 216.

About specifying the Symantec Scan Engine IP address and port for java-based command-line scanner

The -server option lets you specify one or more Symantec Scan Engines for scanning files. If you do not specify a Symantec Scan Engine, the server defaults to the local host that listens on the default port.

The format for each Symantec Scan Engine entry is <IPaddress:port>, where IPaddress is the DNS name or IP address of the computer on which Symantec Scan Engine is running, and port is the port number on which Symantec Scan Engine listens. You only need to specify the port number if Symantec Scan 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 Scan 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 Scan Engine is specified, the load balancing and failover features of the API are activated automatically. The Symantec Scan Engine API provides scheduling across any number of computers that are running Symantec Scan Engine. When multiple Symantec Scan Engines are used, the API determines which Symantec Scan Engine should receive the next file based on the scheduling algorithm.

If a Symantec Scan Engine is unreachable or stops responding during a scan, another Symantec Scan Engine is called. The faulty Symantec Scan Engine is taken out of rotation for 30 seconds. If all of Symantec Scan Engines are out of rotation, the faulty Symantec Scan Engines are called again.

The API does not stop trying to contact Symantec Scan 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

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 Scan 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 Scan Engine tries to repair infected files. Files that cannot be repaired are not deleted.
Scanrepairdelete	Symantec Scan 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 Scan Engine using the Java-based command-line scanner, the command-line scanning mode overrides the scan policy configuration on Symantec Scan 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 the Symantec Scan Engine.

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 216.

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 folowing:

File Scanned: c:\work\filea

Scan Status: Clean

Appendix C

Editing configuration data

This appendix includes the following topics:

- Editing the Symantec Scan Engine configuration files
- How to use the XML modifier command-line tool
- About configuration options

Editing the Symantec Scan Engine configuration files

You can configure most of the options for Symantec Scan Engine through the Web-based console. However, there are configuration options that are not available in the console that you might need to reconfigure.

In Symantec AntiVirus Scan Engine version 4.3 and earlier, you can modify certain settings by editing the configuration file, symcscan.cfg. The format of that configuration file has been converted to Extensible Markup Language (XML) format. The conversion to XML format is handled during installation.

See "Before you install" on page 27.

You can change certain Symantec Scan Engine settings by modifying the data in the XML files.

The XML files that you can modify are as follows:

configuration.xml	Contains logging, the temporary directory location, protocol configurations, and operating-system-specific settings
filtering.xml	Contains settings for URL filtering, MIME, and container limits
liveupdate.xml	Contains LiveUpdate options
policy.xml	Contains access-denied and notification messages, extension policy and extension lists, and Bloodhound scanning settings

In Solaris and Linux, the default location for the XML files is /opt/SYMCScan/bin/. In Windows, the default location is C:\Program Files\Symantec\Scan Engine\ for 32-bit Windows platform, and C:\Program Files (x86)\Symantec\Scan Engine\ for 64-bit Windows platform.

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 editing the XML files, you must stop and restart Symantec Scan 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 Scan Engine daemon on Linux and Solaris" on page 46.

See "Verifying, stopping, and restarting the Symantec Scan Engine service on Windows" on page 47.

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.

How to use the XML modifier command-line tool

Use the XML modifier command-line tool to modify XML files without having to open them in a text editor. Each option requires an XPath argument. You use an XPath argument to specify the node in the XML document that you want to modify.

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 on the product CD. This tool is automatically installed when you install the product.

To access the XML modifier command-line tool

- At the command prompt, type the following:

  java -jar

  xmlmodifier.jar

About option commands

Table C-1 provides the option commands that you can use with the XML modifier command-line tool.

Table C-1 Option commands

Option name	Description
Remove	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 remove option command is as follows: `java -jar xmlmodifier.jar -r XPath XMLfile`
Bulk copy	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 bulk copy command is as follows: `java -jar xmlmodifier.jar -b XPath bulkfile XMLfile`
Node value	This command sets a node value. The value option command is as follows: `java -jar xmlmodifier.jar -s XPath newvalue XMLfile`
Setting a password	This command sets the password that is found in the configuration.xml file to the appropriate encrypted value. The password option command is as follows: `java -jar xmlmodifier.jar -p password configuration.xml`
Testing the password	This command tests the password that is found in the configuration.xml file with the specified value. An output is made to the command-line that indicates whether the passwords are equal. The password test command is as follows: `java -jar xmlmodifier.jar -t password configuration.xml`

Table C-1 Option commands *(continued)*

Option name	Description

Encrypting the password	This command encrypts the specified password and outputs the results to the command-line.
	The password encryption command is as follows:
	`java -jar xmlmodifier.jar -e password`
	where <password> is your password.
	You can use the set (-e) option to set the encrypted value into the file. For example, the following command sets the password to the specified encrypted value:
	`java -jar xmlmodifier.jar -e //admin/password/@value 1F49C564D6F77B2B8E8BEA2D831E6614D3893AE7ADB8D378CBFAF676F0670D0E configuration.xml`

Query	This command returns the value of the node in the XML document with no newline. The query option command is as follows: `java -jar xmlmodifier.jar -q XPath XMLfile`
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 query list command is as follows: `java -jar xmlmodifier.jar -l Xpath XMLfile`

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 to configure the following options:

- Configure the ICAP response
  See "Configuring the ICAP response" on page 224.
- Configure the ICAP preview option
  See "Configuring the ICAP preview option" on page 224.
- Control the dynamic thread pool
  See "Controlling the dynamic thread pool" on page 225.
- Disable the ICAP threshold client notification feature

See "Disabling the ICAP threshold client notification" on page 227.

- Specify the maximum file name lengths
  See "Specifying maximum lengths for file names" on page 228.
- Specify whether to scan top-level files
  See "Specifying whether to scan top-level files" on page 228.
- Configure the number of LiveUpdate retries
  See "Configuring the number of LiveUpdate retries" on page 229.
- Change the LiveUpdate base time
  See "Changing the LiveUpdate base time" on page 229.
- Extract all streams from OLE-structured storage documents for scanning
  See "Extracting all streams from OLE-structured storage documents for scanning" on page 229.
- Specify a replacement file name
  See "Specifying a replacement file name" on page 230.
- Specify archive file types to scan
  See "Specifying archive file types to scan" on page 230.
- Modify the ICAP options attribute-list extension
  See "Modifying the ICAP options attribute-list extension" on page 231.
- Modify the ICAP response to send the non-viral threat category name
  See "Modifying the ICAP response to send the non-viral threat category name" on page 232.
- Access scan error files
  See "Accessing scan error files" on page 232.
- Delete or repair infected read-only files
  See "Deleting or repairing infected read-only files" on page 232.
- Enable non-viral threat categories information
  See "Enabling non-viral threat categories information" on page 234.
- Specify decomposer file size limit
  See "Specifying decomposer file size limit" on page 235.
- Specify maximum file size for extracted files
  See "Specifying maximum file size for extracted files" on page 235.
- Specify maximum cumulative file size for extracted files
  See "Specifying maximum cumulative file size for extracted files" on page 236.
- Specify maximum socket timeout value
  See "Specifying the maximum socket time-out value" on page 236.

Configuring 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 Scan 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-2 lists the ICAP response settings.

Table C-2 ICAP response settings

Xpath	Field values	Default setting
/configuration/protocol/ ICAP/ICAPResponse/@value	■ False Send an access denied message or ICAP 403 response. ■ True Send a replacement file.	True

Configuring 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-3 lists the ICAP preview settings.

Table C-3 ICAP preview settings

Xpath	Field values	Default setting
/configuration/protocol/ icap/ICAPPreviewAll/@value	■ False Send the transfer headers based on the Symantec Scan Engine extension lists. ■ True Send a transfer-preview header indicating preview all.	True

Controlling the dynamic thread pool

The pool of scanning threads that is available to Symantec Scan 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:

MinThreads	The minimum number of scanning threads that is created at start-uptime and the minimum to keep alive regardless of the load that is processed. The default setting is 16. You can increase this number if the default setting of 16 cannot satisfy a typical load. The MinThreads value cannot be greater than the MaxThreads value. (Symantec Scan Engine does not validate the value that you input to ensure that it is lower than the MaxThreads value.) If the MinThreads value is greater than MaxThreads value, Symantec Scan 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.
GrowThreadCount	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 ShrinkThreadCountvalue. Reasonable values are in the range of 0 to 16. **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.

ShrinkThreadCount	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.
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-4 lists the dynamic thread-pool settings.

Table C-4 Dynamic thread-pool settings

Xpath	Field values	Default setting
/configuration/resources/system/MinThreads/@value	Integer between 0 - 512	16
/configuration/resources/system/GrowThreadCount/@value	Integer between 0 - 16	4
/configuration/resources/system/ShrinkThreadCount/@value	Integer between 0 - 16	2
/configuration/resources/system/BusyRequestCount/@value	Integer 0 or greater	4
/configuration/resources/system/IdleThreadCount/@value	Integer between 0 - 16	6

Table C-4 Dynamic thread-pool settings *(continued)*

Xpath	Field values	Default setting
/configuration/resources/system/SecondsBetweenChecks/@value	Integer 2 or greater	5

Disabling the ICAP threshold client notification

Symantec Scan Engine sends a notification to the specified logging destinations when it reaches the scan queued requests threshold. If your client uses ICAP, Symantec Scan 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 Scan 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 Scan Engine" on page 59.

See "ICAP return codes" on page 240.

See "Logging levels and events" on page 159.

Table C-5 lists the threshold client notification settings.

Table C-5 Threshold client notification settings

Xpath	Field values	Default setting
/configuration/protocol/ICAP/EnableServerTooBusyResponse/@value	■ False Disables the ICAP threshold client notification. ■ True Enables the ICAP threshold client notification.	True

Specifying maximum lengths for file names

Use this option to specify the maximum file-name length in bytes. This option only affects the native protocol. A value of 0 (zero) disables this functionality.

Table C-6 lists the maximum file-name limit settings.

Table C-6 Maximum file-name limit settings

Xpath	Field values	Default setting
/configuration/protocol/NATIVE/MaxFilenameLength/@value	Integer 0 or greater Type 0 to disable this functionality.	1024

Specifying whether to scan top-level files

Symantec Scan Engine is configured by default to scan all top-level files. In limited circumstances, you can choose to open top-level files as container files (without scanning) and scan only the contents of the file.

Warning: Change this setting from the default setting only if Symantec Scan Engine provides virus scan and repair services in an email-only environment. In other words, no other types of files are scanned. You can safely bypass the scanning of the top-level file in an email environment. Because it is a container file that is not subject to virus infection. Not scanning top-level files when other types of files are scanned can leave your network vulnerable to virus threats.

Table C-7 lists the top-level scanning settings.

Table C-7 Top-level scanning settings

Xpath	Field values	Default setting
/policies/AntiVirus/ScanTopLevelMIME/@value	■ False Open the top-level file as a container file and scan only the contents of the file (do not scan the top-level file). ■ True Scan all top-level files.	True

Configuring the number of LiveUpdate retries

You can schedule LiveUpdate to run automatically by using the console. Scheduling LiveUpdate to occur automatically at a specified time interval ensures that Symantec Scan Engine always has the most current virus and URL definitions.

See "Configuring LiveUpdate to occur automatically" on page 182.

If LiveUpdate fails, you can configure the number of times Symantec Scan Engine should continue to try to perform a content LiveUpdate.

Table C-8 lists the LiveUpdate retry settings.

Table C-8 LiveUpdate retry settings

Xpath	Field values	Default setting
/liveupdate/schedules/retries/@value	Integer 0 or greater	4

Changing 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 Scan Engine was installed.

See "Configuring LiveUpdate to occur automatically" on page 182.

The LiveUpdate base time is specified in UTC seconds since 00:00:00 January 1, 1970.

Table C-9 lists the LiveUpdate base time settings.

Table C-9 LiveUpdate base time settings

Xpath	Field values	Default setting
/liveupdate/schedules/basetime/@value	Integer 0 or greater	<install time>

Extracting 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 content that can contain viruses. Symantec Scan Engine is configured by default to extract and scan only those streams that are likely to contain viruses. For maximum protection, you can choose to extract and scan all streams. However, performance might be adversely affected depending on the number (and content) of files to be scanned.

Table C-10 lists the OLE-structured storage document scanning settings.

Table C-10 OLE-structured storage document scanning settings

Xpath	Field values	Default setting
/filtering/Container/ Options/ExtractNative OLEStreamsOnly/@value	■ False Extracts all streams. ■ True Extracts only native OLE streams.	True

Specifying a replacement file name

Use this option to specify the name of the attachment file that is returned when Symantec Scan 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-11 lists the replacement file name settings.

Table C-11 Replacement file name settings

Xpath	Field values	Default setting
/filtering/Container/ ReplacementFilename/ @value	Any valid file name	DELETE%.TXT The percentage mark (%) is a sequence number. For example, if two attachments are deleted, the replacement files are called DELETE0.TXT and DELETE1.TXT.

Specifying archive file types to scan

You can specify the types of archive files for which Symantec Scan Engine extracts (decomposes) and scans the internal files.

Note: If the list is empty, Symantec Scan Engine does not scan any archive files.

Table C-12 lists the archive file types to scan settings.

Table C-12 Archive file types to scan settings

Xpath	Field values	Default setting
/configuration/resources/DecEngines/@value	amg, arj, cab, gzip, id, lha, lz, ole1, ss, rar, rtf, tar, tnef, zip, text, mb3, as, bzip2, pdf, mms	zip, ss, gzip, cab, lha, tnef, arj, rar, lz, amg, tar, rtf, text, bzip2, pdf, mms

Modifying the ICAP options attribute-list extension

To list all of the categories that are available for URL filtering, Symantec Scan 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 Scan 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-13 lists the OptBodyAllowed header settings.

Table C-13 OptBodyAllowed header settings

Xpath	Field values	Default setting
/configuration/protocol/ICAP/OptBodyAllowed/@value	■ True Returns the list of categories. ■ False Does not return a list of categories.	True

Modifying the ICAP response to send the non-viral threat category name

You can specify whether you want ICAP to return the name of the non-viral threat in its response when a such a threat is detected. By default, the ICAP response does not send the non-viral threat category name.

Table C-17 lists the EnableNonViralThreatCategoryResp header settings.

Accessing scan error files

By default, Symantec Scan 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 a files that produced an Internal Server Error. This log event is sent to all logging destinations except SSIM and 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-14 lists the AllowAccessOnScanError settings.

Table C-14 AllowAccessOnScanError settings

Xpath	Field values	Default setting
/configuration/protocol/AllowAccessOnScanError/@value	■ False Prohibits access to the files that are blocked by the Internal Server Error result. ■ True Permits access to the files that would normally be blocked by the Internal Server Error result.	False

Deleting or repairing infected read-only files

Symantec Scan 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 Scan Engine can repair or delete infected read-only files. This command applies to all protocols on the Windows platform.

Table C-16 lists the HonorReadOnly settings.

Table C-15 HonorReadOnly settings

Xpath	Field values	Default setting
/policies/Misc/HonorReadOnly/@value	■ False Symantec Scan Engine repairs or deletes the read-only file, if that is the scanning policy. ■ True Symantec Scan Engine does not repair or delete the read-only file, even if that is the scanning policy.	True

Disabling automatic self-test scanning

If your client uses the ICAP protocol or the RPC protocol, Symantec Scan Engine installs with a self-test scanning feature. Symantec Scan Engine performs a test every minute to check whether it is responsive and able to scan files. A test file is sent for Symantec Scan Engine to scan. If Symantec Scan 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 logged to the specified logging destinations.
- You configure Symantec Scan Engine to sends alerts for Warning level events, but you do not want alerts about this event.

See "Logging levels and events" on page 159.

Table C-16 lists the selfscantest settings.

Table C-16 selfscantest settings

Xpath	Field values	Default setting
/configuration/logging/selfscantest/@enabled	■ True Self-scan testing is enabled. ■ False Self-scan testing is disabled.	True

Enabling non-viral threat categories information

The ICAP response headers that Symantec Scan Engine uses indicate the total number of violations that are found in the scanned data. If violations are detected, the header is followed by a series of indented lines that contain information about each violation.

By default, Symantec Scan 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 Scan Engine service.

See "Verifying, stopping, and restarting the Symantec Scan Engine daemon on Linux and Solaris" on page 46.

See "Verifying, stopping, and restarting the Symantec Scan Engine service on Windows" on page 47.

For more information about ICAP response headers, see the *Symantec Scan Engine Software Developer's Guide*.

Table C-17 lists the EnableNonViralThreatCategoryResp settings.

Table C-17 EnableNonViralThreatCategoryResp settings

Xpath	Field values	Default setting
/configuration/protocol/ICAP/EnableNonViral ThreatCategoryResp/@value	■ True Symantec Scan Engine sends the non-viral threat category name. ■ False Symantec Scan Engine does not send the non-viral threat category name.	False

Specifying 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. The `DecFileSize` parameter accepts a value in GB. The maximum top-level container file size that you can specify for tar, rar, and zip containers is 30 GB (~30719 MB). For other containers, you can specify a maximum top-level container file size of 2 GB (~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-18 lists the decomposer file size limit settings.

Table C-18 Decomposer file size limit settings

Xpath	Field values	Default setting
/filtering/Container/ DecFileSize/@value	Integer 0 through 30 Type 0 to disable this setting	2

Note: This parameter does not limit the size of individual files extracted from the top-level container file.

Specifying maximum file size for extracted files

Use this parameter to specify the maximum file size for the individual files that can be extracted on disk and in memory. 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 (~30 GB). For other containers, you can specify a maximum extract file size of 1907 MB (~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-19 lists the extracted file size settings

Table C-19 Maximum file size for extracted files

Xpath	Field values	Default setting
/filtering/Container/ MaxExtractSize/@value	0 through 30719 Type 0 to disable this setting	100

Specifying maximum cumulative file size for extracted files

Use this parameter to specify the maximum cumulative file size for extracted files. Symantec Scan 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 (~30 GB). A value of zero (0) disables this optimization setting.

Table C-20 lists the maximum cumulative file size for extracted files.

Table C-20 Maximum cumulative file size for extracted files

Xpath	Field values	Default setting
/filtering/container/ MaxCumulativeExtractSize/ @value	Accepts value in bytes Type 0 to disable this setting.	0

Specifying the maximum socket time-out value

Typically, a client sends a file to Symantec Scan Engine to scan over a socket and Symantec Scan 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 Scan 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 time-out, a socket time-out error gets generated. You can specify a larger socket time-out value to avoid the socket time-out error.

The maximum socket time-out value that you can enter is 4320 minutes (72 hours) while the default value is 5 minutes.

Table C-21 lists the maximum socket time-out value.

Table C-21 Maximum socket time-out value

Xpath	Field values	Default setting
/configuration/resources/system/SocketTimeOut/@value	Accepts value in minutes	5

Appendix D

Return codes

This appendix includes the following topics:

- Native protocol return codes
- ICAP return codes
- RPC protocol return codes

Native protocol return codes

The following return codes are generated for the native protocol:

- 200 Command okay.
- 201 Output file available.
- 203 Local output file available.
- 220 Symantec Scan Engine ready.
- 221 Service closing transmission channel.
- 230 File scanned.
- 420 Service not available, closing transmission channel.
- 430 File not acceptable at this time.
- 500 Syntax error, command unrecognized.
- 501 Syntax error in parameters.
- 502 Command not implemented.
- 503 Bad sequence of commands.
- 504 Unsupported protocol version.
- 530 File not acceptable.

- 531 File unscannable.
- 532 Output file unavailable.
- 533 Error scanning file.
- 534 File name exceeds configured length.
- 535 Maximum Extract Time exceeded - scan incomplete.
- 536 Maximum Extract Depth exceeded - scan incomplete.
- 537 Maximum Extract Size exceeded - scan incomplete.
- 538 Malformed container file found. File not scanned.
- 539 Aborted - no antivirus scanning license.

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.
- 405 Method not implemented.
- 408 Request timeout.
- 500 Internal server error.
- 503 Service unavailable/overloaded.
- 505 ICAP version not supported.
- 506 Server too busy.
- 533 Error scanning file.
- 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

Glossary

action	The product's response to a policy violation.
alert	An automatic notification that an event or error has occurred.
bind	The process of attaching a network listener to a locally-bound IP address. When you bind a network service to an IP address, Symantec Scan Engine uses this address to listen on, and to transmit data to and from the client.
client	A program that makes requests of or transmits data to a parent server program.
client application	An application that is configured to pass files to Symantec Scan Engine for scanning.
communications protocol	A set of rules that are designed to let computers exchange data. A communications protocol defines issues such as transmission rate, interval type, and mode. See also ICAP, native protocol, and RPC protocol.
console	A program interface for the management of software.
URL category	A pre-defined category provided with Symantec Scan Engine that consists of URLs.
definition file	A file that contains viral and non-viral definitions. You can obtain updated definition files using LiveUpdate or Intelligent Updater. Symantec Scan Engine uses the most current definition file that is available for scanning.
definitions	The content that contains necessary information to detect and eliminate risks, such as viruses and adware. Definitions can also include new URL categories.
denial-of-service attack	Container files that are overly large or that contain large numbers of embedded, compressed files that are designed to overload your system and maliciously use resources and degrade performance. To reduce your exposure to denial-of-service attacks, you can impose limits to control how Symantec Scan Engine handles container files.
encrypted attachment	A message attachment that has been converted into a form that Symantec Scan Engine cannot scan. You to choose an action to take when an encrypted attachment is detected.
event	A significant occurrence in a system or application that a program detects. Events typically trigger actions, such as sending a user notification or adding a log entry.
extension	A suffix consisting of a period followed by several letters at the end of a file that, by convention, indicates the type of the file.

filter	A method for analyzing files, messages, or URLs.
filter policy	A set of actions that apply to a category of messages, URLs, and files.
ICAP (Internet Content Adaptation Protocol)	A lightweight protocol for executing a remote procedure call on HTTP messages. Symantec Scan Engine supports version 1.0 of ICAP, as presented in RFC 3507 (April 2003).
incoming requests	Content from Web sites that is being passed to the user.
IP (Internet Protocol)	The method or protocol by which data is sent from one computer to another on the Internet. Each computer (known as a host) on the Internet has at least one address that uniquely identifies it to all other computers on the Internet.
IP address	A unique number that identifies a workstation on a TCP/IP network and specifies routing information. Each workstation on a network must be assigned a unique IP address, which consists of the network ID, plus a unique host ID assigned by the network administrator. This address is usually represented in dot-decimal notation, with the decimal values separated by a period (for example 123.45.6.24).
list box	A dialog box containing a list of items from which a user can choose.
local categories	A custom category that you create that consists of URLs that contain related subject matter.
multi-homed	A system or server or computer that hosts multiple network interface cards.
native protocol	Symantec Scan Engine's own protocol. The native protocol is a simple TCP/IP protocol. It is text-based like HTTP or SMTP. It uses standard ASCII commands and responses to communicate between the client and the server.
notification	An email that can be automatically sent to the sender, to the recipients, or to other email addresses when a specified condition is met. For example, if you have a policy that removes .exe attachments from incoming messages, you can notify the sender that the attachment has been removed.
outbreak	When a certain 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 a potential outbreaks. This lets you can take the necessary precautions to protect your network.
parameter	A value that is assigned to a variable. In communications, a parameter is a means of customizing program (software) and hardware operation.
policy	A set of instructions that Symantec Scan Engine implements on a file, Web content, or email messages. You can also set policies for scanning.
protocol	A set of rules for encoding and decoding data so that messages can be exchanged between computers. These rules also ensure that each computer reliably use the data. On the Internet, the exchange of information between different computers is made possible by the suite of protocols known as TCP/IP. Protocols can be

	stacked, meaning that one transmission can use two or more protocols. For example, an FTP session uses the FTP protocol to transfer files, the TCP protocol to manage connections, and the IP protocol to deliver data. See also ICAP, native protocol, and RPC protocol.
proxy	An application (or agent) that runs on the security gateway and acts as both a server and client, accepting connections from a client and making requests on behalf of the client to the destination server. There are many types of proxies, each used for specific purposes. See also proxy server.
quarantine	The location where files that are suspected of containing viruses can be isolated. Quarantined files can be forwarded to Symantec Security Response for analysis. If a new threat is discovered, updated definitions are returned automatically.
risk	1. An event that can compromise your network security. 2. A threat (such as a virus, worm or Trojan horse) or a security risk (such as adware and spyware).
RPC (Remote Procedure Call)	A proprietary scanning protocol that uses the MS-RPC protocol to communicate with client applications. This option is not available for Solaris or Linux.
scanner	The components in Symantec Scan Engine that filter email, files, and Web content.
security	The policies, practices, and procedures that are applied to information systems. Securing your information systems ensures that the data that is communicated among and maintained within those systems is not vulnerable to inappropriate or unauthorized use, access, or modification. It also ensures that the networks that are used to store, process, or transmit information are kept operational and secure.
security risk	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
SSL certificate	An electronic, digital certificate that authenticates the identity of the server. SSL certificates are typically signed by an independent, trusted third party. The certificate lets the browser verify the authenticity of the server before it permits the SSL session to begin.
threat	1. A virus, worm, mass-mailer worm, or Trojan horse. 2. A circumstance, event, or person with the potential to cause harm to a system in the form of destruction, disclosure, modification of data, or denial-of-service. See also virus.
time-out	A predetermined period of time during which a given task must be completed. If the time-out value is reached before or during the execution of a task, the task is canceled.

toolbar In the Symantec Scan Engine console, the row below the menu bar containing buttons for a commonly used commands.

true file type recognition A technology that identifies the actual type of a file, whether or not the file extension matches that type.

unscannable A file that cannot be scanned by Symantec Scan Engine for any reason. For example, encrypted files are unscannable.

URL (Uniform Resource Locator) A string of alphanumeric characters that specify an Internet resource. For example:

http://symantecexample.com/news

A URL consists of the protocol (http), the domain name of the computer on which the information is stored (symantecexample.com), and the location of the content (news).

virus A piece of programming code inserted into other programming to cause some unexpected and, for the victim, usually undesirable event. Viruses can be transmitted by downloading programming from other sites or be present on a diskette. The source of the file you are downloading or of a diskette you have received is often unaware of the virus. The virus lies dormant until circumstances cause the computer to execute its code. Some viruses are playful in intent and effect, but some can be harmful, erasing data or causing your hard disk to require reformatting. See also threats.

Web browser A client program that uses the Hypertext Transfer Protocol (HTTP) to make requests of Web servers throughout the Internet on behalf of the browser user.

worm A special type of virus. A worm does not attach itself to other programs like a traditional virus, but creates copies of itself, which create even more copies. See also threat and virus.

WWW (World Wide Web) An application on the Internet that allows for the exchange of documents formatted in Hypertext Markup Language (HTML), which facilitates text, graphics, and layout. As the World Wide Web has grown in popularity, its capabilities have expanded to include the exchange of video, audio, animation, and other specialized documents. The World Wide Web is also a system of Internet servers that support specially formatted documents. Another important aspect of the World Wide Web is the inclusion of hypertext links that allow users to click links and quickly navigate to other related sites.

Index

Symbols

.zip files. *See* container files

A

ActiveX 95
administrator settings
    password 56
    timeout 56
Adobe Acrobat Reader 15
adware. *See* security risks
alerts 170
    See also logging
    about 170
    intervals, maximum load 59
    outbreak notifications 173
    SMTP 170
    SNMP 171
antivirus. *See* threats

B

bind address
    console 56
    ICAP 80
    log 162
    native protocol 83

C

certificate file 54
Certificate Import Utility 54
command-line scanner
    about 201
    file scanning 202
    installing 202
    IP address and port 206
    options 204
    recursive scanning 211
    redirecting console output 212
    scanning mode 207
    scanning results 208
    supported platforms 202
command-line scanner *(continued)*
    supported protocol 202
    syntax and usage 203
configuration data 219
configuration.xml 219
console 219
    See also XML modifier command-line tool
    accessing 49
    configuring interface settings 56
    password 56
    port 56
    server address 56
    SSL port 56
    time-out 56
container files
    blocking unscannable 103
    setting processing limits 129
content categories 147
    See also HTTP filtering
    See also local categories
content license 69

D

DBCS path names 203
definitions
    about 179
    Rapid Release 190
    types 179
    updating
        using Intelligent Updater 187
        using LiveUpdate 182
dynamic thread pool 59

E

email, filtering by
    file name 105
    file or attachment size 107
    maximum mail size 128
    message origin 110
    subject 108
events, logging 159

F

filtering. *See* HTTP filtering and email, filtering by
filtering.xml 219
fulfillment ID 73

H

Home page components 50
HTTP filtering
    about 134
    customizing the access denied message 155
    local categories 147
    modes 149
    URL categories 134
HTTPS server 53

I

ICAP
    about 79
    bind address 80
    command-line scanner, using 201
    configuring 80
    port number 80
    quarantining unrepairable files 99
    return codes 240
    scan policy 80
    supported services 76
installation
    command-line scanner 202
    on Linux 38
    on Solaris 42
    on Windows 33
    preparing for 27
Intelligent Updater
    about 187
    definition file size 187
    definitions, Symantec update frequency 180
    enabling 188

J

JRE (Java Runtime Environment) 15, 27

K

keys 53
keystore 53

L

license
    content 73
    content license 69
    locating the serial number 71
    product 73
    product license 69
licensing
    about 69
    activating 70
    checking status 73
    license file
        installing 72
        obtaining 71
        removing 73
    types of licenses 69
Linux
    installing Symantec Scan Engine 38
    stopping and starting service 46
    system requirements 30
    uninstalling 67
LiveUpdate
    about 182
    configuring LiveUpdate server 184
    definitions, Symantec update frequency 180
    licensing requirement 69
    rolling back definitions 192
    updating definitions
        automatically 182
        on demand 183
LiveUpdate Administration Utility 15
liveupdate.xml 219
load 119
load balancing 20
local categories 147
    See also content categories
    See also HTTP filtering
    about 147
    managing 151
local logging
    configuring 164
    exporting data 176
    managing local logs 174
    purging log files 166
    statistics reporting 167
    viewing data 175
logging 170
    See also alerts
    about 157

logging *(continued)*
changing log file location 164
configuring local logging 163
destinations 157
levels and events 159
outbreak alerting 173
purging log files 166
reporting functions 174
SMTP alerts 170
SNMP alerts 171
statistics reporting 167
viewing statistic logs data 176
Windows Event Log 168

M

mail filter policy, blocking by
file name 105
individual file size 107
mail subject 108
message origin 110
total file or message size 128
mail message update feature 105

N

native protocol
about 82
bind address 83
configuring 83
port number 83
return codes 239
supported services 76
notifications
configuring 163
logging 157

O

outbreak alerts 173

P

PFX certificate file 54
PKCS#12 certificate file 54
policy.xml 219
port number, configuring
console 56
ICAP 80
native protocol 83
POST transactions 79, 100
process priority 119
processing limits 129
product
license 69, 73
protection, updating
Rapid Release 190
using Intelligent Updater 187
using LiveUpdate 182
protocol
ICAP 84
native 82
RPC 84
supported protocols 75
supported services 76

Q

Quarantine 99
queue size 59

R

Rapid Release
about 190
updating definitions
automatically 191
on demand 192
recursive scanning 211
resource 119
resource consumption 119
return codes
ICAP 240
native protocol 239
RPC 241
risks. *See* threats and security risks
RPC
client IP address 87
configuring 84
notifying server of updated definitions 90
notifying users of threat detection 114
quarantining unrepairable files 99
return codes 241
supported services 76

S

scanning 208
See also command-line scanner
See also HTTP filtering
See also threats
improving performance 125, 128
scanning thread 119

scans
licensing requirements 69, 73
specifying temporary scanning directory 59
security risks
categories of 100
detecting 100
self-test scanning 233
serial number 71
service startup properties
editing 92
silent installation
creating response file 194
generating encrypted password 200
initiating installation
Linux and Solaris 197
Windows 199
installing
Linux and Solaris 193
Windows 197
SMTP alerts
alert bind address 162
configuring 170
SNMP alerts
alert bind address 162
configuring 171
Solaris
installing Symantec Scan Engine 42
stopping and starting service 46
system requirements 29
uninstalling 67
spyware. *See* security risks
SSIM
Symantec Security Information Manager 169
SSL (Secure Socket Layer) 53
Symantec Scan Engine
allocating resources 59
configuring using XML modifier command-line tool 219
installing 32
new features 14
running other antivirus software 28
starting and stopping the daemon 46
starting and stopping the service 47
types of risks detected 95
Symantec Security Information Manager. *See* SSIM
Symantec Security Response 190
symcscan.cfg 64
system requirements 28

T

temporary scanning directory
specifying 59
third-party certificate 53
thread pool
maximum threads 59
XML modifier command-line tool 225
threats 95, 129
See also command-line scanner
See also container files
blocking by
file name 105
individual file size 107
mail subject 108
message origin 110
blocking unscannable files 103
enabling detection 97
quarantining infected files 99
testing detection capabilities 98

U

uninstallation 67
upgrade 27, 64
URL (Uniform Resource Locator) 133
URL categories
about 134
denying access 150
overriding a URL categorization 154
predefined categories 134
URL filtering
about 134
customizing the access denied message 155
local categories 147
See also
modes 149
URL categories 134
user notifications
customizing 111, 155
RPC-client users 114
UTF-8 encoding 108, 150, 219

V

virus 95, 129
See also command-line scanner
See also container files
blocking by
file name 105
individual file size 107

virus *(continued)*
blocking by *(continued)*
mail subject 108
message origin 110
blocking unscannable files 103
enabling detection 97
quarantining infected files 99
testing detection capabilities 98

W

Windows
installing Symantec Scan Engine 33
system requirements 29
uninstalling 67
Windows 2000 Server/Server 2003
stopping and starting service 47
Windows Event Log 168

X

XML modifier command-line tool
accessing 220
configuration options 222
file locations 219
using 220
XPath argument 220