Symantec Scan Engine 5.1

This document includes the following topics:

About Symantec Scan Engine

Symantec™ Scan Engine, formerly marketed as Symantec AntiVirus™ 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 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 6.

The Symantec Scan Engine software development kit (SDK) lets you develop custom integrations. It supports version 1.0 of ICAP, as presented in RFC 3507 (April 2003). Symantec also has developed connector code for some third-party applications for seamless integration with Symantec Scan Engine.

What's new

Table 1-1 describes the new features in Symantec Scan Engine 5.1.

Table 1-1 New features

Feature	Description
Scanning for security risks	Symantec Scan Engine can detect security risks for clients that use ICAP. Security risks include, but are not limited to, adware, dialers, hack tools, joke programs, remote access programs, spyware, and trackware.
Additional operating system support	Symantec Scan Engine supports Solaris 10 (with a SPARC® processor only).
Ability to perform silent upgrades	You can perform silent upgrades for the supported operating systems.

Table 1-1 New features (Continued)

Feature	Description
Certificate Import Utility	Symantec Scan Engine secures the HTTPS and SSL servers with public and private keys, which it creates when you install the product. To enhance security, Symantec Scan Engine provides a utility that lets you import keys from third-party certificates. This utility is automatically installed when you install Symantec Scan Engine.
Support for SESA 2.5	Symantec Scan Engine supports logging events to the Symantec Enterprise Security Architecture (SESA) version 2.5. SESA is seamlessly integrated with Symantec Incident Manager, the software component for the Symantec Security Information Manager appliance. Together, these tools provide you with an open, standards-based foundation for managing security events from Symantec clients, gateways, servers, and Web servers.

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\
Silent installation	The files that you can use to perform a silent installation or upgrade. Also includes response files for Red Hat and Solaris.	Silent_Install\
Command-line scanner	The software that acts as a client to Symantec Scan Engine through 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\

Table 1-2 Product components (Continued)

Component	Description	Folder name
Symantec Scan Engine software developer's kit	The tools and information that you can use to create customized integrations using ICAP.	Scan_Engine_SDK\
Symantec Central Quarantine server	The tool that lets you quarantine infected files that cannot be repaired when you use the ICAP or RPC protocol. Symantec Central Quarantine server lets you isolate unrepairable files so that threats cannot spread.	Tools\Central_Quarantine\
LiveUpdate™ Administration Utility	The utility that lets you 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 directly from Symantec or from a LiveUpdate server. For more information, see the *LiveUpdate Administrator's Guide* on the product CD.	Tools\LiveUpdate_Admin\
Java™ 2SE Runtime Environment (JRE) 5.0 Update 6	The software that lets you access the Symantec Scan Engine console.	Java\
SESA Agent installer	The program that lets you install the SESA Agent, which handles the communications between Symantec Scan Engine and Symantec Enterprise Security Architecture (SESA). SESA is an event management system that uses data collection services for events that Symantec and supported third-party products generate.	Tools\SESA_Agent_Installer\

Table 1-2 Product components (Continued)

Component	Description	Folder name
SESA Integration package	The tools that extends SESA functionality to include Symantec Scan Engine event data.	Tools\SESA_SIPI_Installers\SSE
Adobe® Acrobat® Reader® 7.0	This is the software that makes it possible to read electronic documentation in Portable Document Format (PDF).	Adobe_Reader\
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. For Windows® platforms only.	Technical_Support\Win2K\

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 simple TCP/IP protocol to provide scanning functionality to client applications. This protocol is text-based, like HTTP or SMTP. It uses standard 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 subsequent files.
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 (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.
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 by letting the application be distributed over multiple platforms. The use of RPC frees the developer from having to be familiar with various operating system and network interfaces. RPC simplifies the development of applications that span multiple operating systems and network protocols. It reduces complexity by keeping the semantics of a remote call the same regardless of whether the client and server are located 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/Server 2003. Any appropriate client can use RPC to communicate with Symantec Scan Engine to request the scanning and repairing of files.

Before you install

Install Symantec Scan Engine on a computer that meets the system requirements. Ensure that you install and configure the operating system software and applicable updates for your server (and that they are working correctly) before you install Symantec Scan Engine. For more information, see the documentation for your server.

See "System requirements" on page 8.

Java™ 2SE Runtime Environment (JRE) 5.0 Update 6 or later (within the version 5 platform) must be installed on the server before you install Symantec Scan Engine. If you need to install JRE 5.0 Update 6, it is included on the product CD in the following location:

\Java\<operating system platform>

Prior to installing Symantec Scan Engine, you must 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 "Running other antivirus products on Symantec Scan Engine server" on page 7.

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

See "Post-installation tasks" on page 13.

Running other antivirus products on Symantec Scan Engine server

By design, Symantec Scan Engine scans only the files from client applications that are configured to pass files to Symantec Scan Engine. Symantec Scan Engine does not protect the computer on which it runs. Because the server on which Symantec Scan Engine runs processes files that might contain threats, the server is vulnerable if it has no real-time threat protection.

To achieve comprehensive protection with Symantec Scan Engine, you must protect the Symantec Scan Engine server from attacks by installing an antivirus program such as Symantec AntiVirus™ Corporate Edition on the server that runs Symantec Scan Engine.

Note: To prevent a conflict between Symantec Scan Engine and the antivirus product that is running on the host computer, you must configure the antivirus product on the host computer so that it does not scan the temporary directory that Symantec Scan Engine uses for scanning.

System requirements

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

Windows 2000 Server/Server 2003 system requirements

The following are the system requirements for Windows 2000 Server/Server 2003:

Operating system	■ Windows 2000 Server with the most current service pack ■ Windows Server 2003 (32-bit)
Processor	Pentium 4 processor 1 GHz or higher
Memory	512 MB of RAM or higher
Disk space	500 MB of hard disk space
Hardware	■ 1 network interface card (NIC) running TCP/IP with a static IP address ■ Internet connection to update definitions
Software	■ J2SE Runtime Environment (JRE) 5.0 Update 6 or later (within the version 5 platform) installed JRE 5.0 Update 6 is provided on the product CD in the following folder: Java\Win2K ■ Microsoft Internet Explorer 6.0 (with the most recent service pack that is available) Internet Explorer is only required for Web-based administration. Internet Explorer must be installed 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 (primary) Ensure that your operating system has the most recent patches that are available.
Processor	SPARC® 400 MHz or higher
Memory	512 MB of RAM or higher
Disk space	500 MB of hard disk space
Hardware	■ 1 network interface card (NIC) running TCP/IP with a static IP address ■ Internet connection to update definitions
Software	■ J2SE Runtime Environment (JRE) 5.0 Update 6 or later (within the version 5 platform) installed JRE 5.0 Update 6 (self-extracting) is provided on the product CD in the following folder: 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. ■ Microsoft Internet Explorer 6.0 (with the most recent service pack that is available) Internet Explorer is only required for Web-based administration. Internet Explorer must be installed 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 Enterprise Linux 3.0 ■ Red Hat Linux Advanced Server 2.1 ■ SuSE Linux Enterprise Server 9
Processor	Pentium 4 processor 1 GHZ or higher
Memory	512 MB of RAM or higher
Disk space	500 MB of hard disk space

Hardware	■ 1 network interface card (NIC) running TCP/IP with a static IP address ■ Internet connection to update definitions
Software	■ J2SE Runtime Environment (JRE) 5.0 Update 6 or later (within the version 5 platform) installed JRE 5.0 Update 6 for Red Hat is provided on the product CD in the following folder: Java\Red Hat 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. ■ Microsoft Internet Explorer 6.0 (with the most recent service pack that is available) Internet Explorer is only required for Web-based administration. Internet Explorer must be installed 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, and then it does one of the following:

No previous version is detected.	A full installation is performed.
Version 5.0x or 4.3x is detected.	Symantec Scan Engine supports upgrades from version 4.3x. If an upgrade is possible, 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 5.1" on page 11.

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

During installation, Symantec Scan Engine installs a virtual administrative account. Do not forget the password for this account because it is the only account that you can use to manage Symantec Scan Engine. You can change the password in the console, but to do so you must have the old password.

After you install Symantec Scan Engine, you must activate all applicable licenses. You can also configure LiveUpdate to automatically receive definition updates. These features are not updated until you activate the appropriate licenses.

If you are upgrading from a previous version that has valid licenses, when the installation is complete, Symantec Scan Engine automatically recognizes these licenses. For information about licensing, see the *Symantec Scan Engine Implementation Guide*.

If Symantec Scan Engine fails to start before it can initiate standard logging (for example, if the XML configuration does not validate), information about the failure is written to the abort log file, ScanEngineAbortLog.txt. This file is located in the installation directory.

If you are installing or upgrading multiple Symantec Scan Engines on your network, you can use the silent installation or upgrade feature to facilitate the process.

For installation procedures, see the *Symantec Scan Engine Implementation Guide*.

Migrating to version 5.1

Symantec Scan Engine supports upgrades from version 4.3x. If you are upgrading from version 5.x, Symantec Scan Engine retains all of the settings and values that you have configured.

If you are upgrading from version 4.3x of Symantec AntiVirus Scan Engine, you can install the upgrade over the existing installation (without first uninstalling the previous version). Installing the upgrade over the existing installation retains most, but not all, of the customizations that you have made to the files and message catalogs. The format of the configuration files has changed since the 4.3x release. The transfer to the Extensible Markup Language (XML) format is handled during installation.

Note: If you are upgrading 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) when you upgrade from a previous version or perform a new installation.

Table 1-4 provides information about how the configuration files are affected after an upgrade from version 4.3x.

Table 1-4 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 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. **Note:** Scan engine 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 5.1. 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 just mail files. If you had a mail policy in effect, check the configuration through the Symantec Scan Engine console after the upgrade is complete.
Domains.cfg	This file is not used in version 5.1. 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 reference the file to reconfigure the blacklist after the upgrade.

Table 1-4 Configuration files that are affected after an upgrade (Continued)

File or message catalog	Description
Symcsmsg.dat	This file is not used in version 5.1. 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 5.1 use a different format, so data from previous log files are not included in the reports that are generated in version 5.1.

Post-installation tasks

After you have installed Symantec Scan Engine, you can perform the following post-installation tasks:

- Verify that the Symantec Scan Engine daemon is running on Linux and Solaris
- Enhance security for the HTTPS and SSL servers
- Clear the Java cache
- Access the console
- Install the appropriate licenses
- Change the administrator settings
- Allocate resources for Symantec Scan Engine

For more information about performing the post-installation tasks, see the *Symantec Scan Engine Implementation Guide*.

Where to get more information about Symantec Scan Engine

The *Symantec Scan Engine Implementation Guide* provides information about using this product and is on the product CD in the following location:

Scan_Engine\Docs\

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.securityresponse.symantec.com

04/06 PN: 10493980