Symantec AntiVirus™ for Network Attached Storage Integration Guide
Symantec AntiVirus™ for Network Attached Storage Integration Guide

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

Documentation version: 5.2.13

Legal Notice

Copyright © 2011 Symantec Corporation. All rights reserved.

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

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

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

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

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

This document includes the following topics:

■ About Symantec AntiVirus for Network Attached Storage
■ What’s new in 5.2.13
■ How to use the Symantec AntiVirus for Network Attached Storage documentation
■ Why you need virus protection in a network attached storage environment
■ About preparing for installation
■ Post-installation tasks

About Symantec AntiVirus for Network Attached Storage

Symantec AntiVirus™ for Network Attached Storage provides virus scanning and repair services for a number of network-attached storage (NAS) devices. Symantec AntiVirus for Network Attached Storage features the Symantec™ Scan Engine, a carrier-class virus scanning and repair engine. The Symantec Scan Engine features all of the virus-scanning technologies that are available in Symantec antivirus products, making the Symantec Scan Engine one of the most effective virus solutions available for detecting and preventing virus attacks.
You can scan files for viruses automatically as they are accessed from storage before the requesting user gains access to it. Based on a configurable virus scan policy, when a virus is found in a file, the file is repaired. The clean file is stored on the NAS device and only then is the requesting user granted access.

Symantec Scan Engine uses the following protocols to interface with network-attached storage devices:

- The Internet Content Adaptation Protocol (ICAP), version 1.0, as presented in RFC 3507 (April 2003)

- A proprietary implementation of remote procedure call (RPC)

- The scan engine native protocol

Each NAS device maintains a connection with Symantec Scan Engine to request scanning and repairing of files.

**About software components**

In most cases, adding virus scanning to a supported NAS device requires installation and configuration of the following components:

- Symantec Scan Engine, which provides the virus scanning and repair services
  See “About Symantec Scan Engine” on page 9.

- Connector, which lets the NAS device communicate with Symantec Scan Engine
  See “About the connector” on page 10.

The connector handles the communication between the scan engine and the NAS device and interprets the results that are returned from the scan engine after scanning. The manufacturer of the NAS device develops and provides support to the connector. The connector typically is installed and configured on the NAS device. (In some cases, the manufacturer pre-installs the connector.)

**Figure 1-1** shows a typical integration of a network-attached storage device with Symantec Scan Engine.
Figure 1-1 Integration of a network attached storage device with the Symantec Scan Engine

1. The client tries to access a file on the network attached storage device.
2. The network attached storage device, by means of a connector, sends the file to the Symantec Scan Engine for scanning.
3. Symantec Scan Engine scans the file, repairs it if it is infected, and returns the clean file to the network attached storage device.
4. The network attached storage device writes the cleaned file to disk, caches the fact that the file has been cleaned, and sends the file to the client.

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:

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

Symantec Scan Engine is included in the Symantec AntiVirus for Network Attached Storage distribution package.
For more information about the scan engine, see the *Symantec Scan Engine Implementation Guide* on the product CD.

**About the connector**

The connector handles the communication between the scan engine and the NAS device and interprets the results that are returned from the scan engine after scanning. The manufacturer of the NAS device develops and provides support for the connector. The connector typically is installed and configured on the NAS device. (In some cases, the manufacturer pre-installs the connector.)

In some cases, no connector is necessary. The NAS device handles the communication with the scan engine, and any configuration options are available directly on the device.

**What's new in 5.2.13**

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

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
</table>
| Windows Active Directory-based Authentication mode | You can now access the Symantec Scan Engine console using the following two types of authentication modes:  
* Symantec Scan Engine-based authentication mode This legacy authentication method requires users to enter the Symantec Scan Engine administrator password to access the console.  
* Windows Active Directory-based authentication mode Only users from the authorized Windows Active Directory security group can access the Symantec Scan Engine console using their Active Directory credentials. |

**Note:** For non-Windows platforms, users only have the Symantec Scan Engine-based authentication mode for accessing console.
How to use the Symantec AntiVirus for Network Attached Storage documentation

To configure Symantec AntiVirus for Network Attached Storage to work with one of the supported NAS devices, you need the documentation that is included in the Symantec AntiVirus for Network Attached Storage distribution package. You need the documentation that is provided by the manufacturer of the NAS device as well.

The Symantec AntiVirus for Network Attached Storage distribution package includes the following documents:

- Symantec Scan Engine Implementation Guide
- Symantec AntiVirus for Network Attached Storage Integration Guide
- Configuration guides for Symantec certified Network Attached Storage devices

The manufacturer of the NAS device develops the connector to integrate Symantec Scan Engine. The manufacturer of the NAS device also prepares and distributes supporting documentation for the connector. Obtain the connector and any supporting documentation from the manufacturer if you do not receive it with the NAS device.

About the Symantec Scan Engine Implementation Guide

Use the Symantec Scan Engine Implementation Guide as the primary guide for installing and configuring Symantec Scan Engine. This guide contains the information that you need to consider about the scan engine configuration options.

About the Symantec AntiVirus for Network Attached Storage Integration Guide

The Symantec AntiVirus for Network Attached Storage Integration Guide provides an overview of how Symantec Scan Engine and the Network Attached Storage device interact during virus scanning. It also explains why you need virus protection in a network attached storage environment.

About configuration guides for Symantec certified Network Attached Storage devices

Use the guidance and recommendations that are in these guides with the manufacturer-prepared documentation to implement virus scanning.

Each of these guides includes the following information:
General information on how antivirus scanning works with the NAS device
Information for configuring the scan engine to work with the NAS device
Information on configuring the NAS device to work with the scan engine
Known issues

For the latest supported network attached storage device documentation, see http://www.symantec.com/docs/TECH147442

Why you need virus protection in a network attached storage environment

Network attached storage provides many benefits, such as increased performance, heterogeneous data access, data redundancy, ease of storage management, and real-time backup recovery. However, the implementation of a NAS system introduces security risks that should be addressed. Data can be accessed and compromised more quickly when it is consolidated into a centralized NAS system. This occurs because NAS systems are typically connected directly to the local network.

Installing virus protection software at key locations in the corporate network is not sufficient to protect data on NAS servers. Examples of such key locations are firewalls, email gateways, and desktops.

Dedicated antivirus protection for a NAS system should be part of a comprehensive security policy for the following reasons:

- Storage servers are susceptible to attacks from viruses, worms, Trojan horses, and other malicious code because large number of users access them and they contain large amounts of data.
- Malicious code can result in lost, stolen, or corrupted files, which can result in costly downtime to the enterprise.
- The NAS system can become a vector for the malicious code when a threat is stored on the NAS system. It can compromise the computers and the data of the users who access the NAS system.
- Malicious code can be replicated multiple times in multiple locations through NAS backup, mirroring of data, and archiving. The malicious code can be re-introduced to the NAS system when NAS data that contains malicious code is restored from one of these locations. This re-introduction can potentially reinfect the network.
- Malicious code could replicate on the NAS system in multiple locations and infect other parts of the network. The effort to remove a threat becomes a
time-consuming task that involves significant downtime as well as time and money for data recovery.

■ The NAS system can be used as an access point to the rest of the network or as a launch point for an attack. For example, a denial-of-service attack can be launched in a NAS system.

■ Industry regulations and laws now require that organizations that maintain financial, medical, personal, and email data should protect the data from being stolen, altered, or destroyed. Organizations are legally responsible for providing comprehensive protection for stored data.

How the scan engine protects against viruses

Symantec Scan Engine detects viruses, worms, and Trojan horses in all major file types (for example, Windows files, DOS files, and Microsoft Word and Excel files). Symantec Scan Engine includes a decomposer that handles most compressed and archive file formats and nested levels of files. You can configure the scan engine to limit scanning to certain file types by a file extension and file type exclusion list.

Symantec Scan Engine provides protection against those container files that can cause denial-of-service attacks. Examples are those container files that are overly large, that contain large numbers of embedded compressed files, or that have been designed to use resources maliciously and degrade performance. You can specify the maximum amount of time that the scan engine devotes to extracting a file and its contents, the maximum file size for container files, and the maximum number of nested levels to be decomposed for scanning.

Symantec Scan Engine also detects mobile code such as Java™, ActiveX®, and standalone script-based threats. Symantec Scan Engine uses Symantec antivirus technologies, including Bloodhound™, for heuristic detection of new or unknown viruses; NAVEX™, which provides protection from new classes of viruses automatically through LiveUpdate; and Striker, for the detection of polymorphic viruses.

The scan engine can also be configured to send alerts when specific thresholds are met or exceeded. For example, if the same type of virus has been detected ten times in a 20-minute interval, the scan engine can be configured to send an alert to any of the scan engine logging or alerting destinations.

About Symantec Security Response

Symantec Scan Engine is supported by the Symantec Security Response team. These Symantec engineers work 24 hours per day, 7 days per week, tracking new virus outbreaks and identifying new virus threats.
For more information about protection against a specific virus, visit the Symantec Security Response Web site at: http://securityresponse.symantec.com

For more information, see the Symantec Scan Engine Implementation Guide.

About preparing for installation

Before you install Symantec Antivirus for Network Attached Storage, you should ensure that your computer meets the system requirements for installing the scan engine. The scan engine is included on the Symantec AntiVirus for Network Attached Storage CD.

If the scan engine uses RPC protocol to interface with your network attached storage device, Symantec Scan Engine must be installed on Windows 2000 Server/Windows 2003 Server/Windows 2008 Server platforms only.

For more information about installing the scan engine, see the Symantec Scan Engine Implementation Guide on the product CD.

Windows system requirements

The following are the system requirements for installing Symantec AntiVirus for Network Attached Storage on a Windows 2000 Server/Windows 2003 Server/Windows 2008 Server:

- **Operating system**
  - Windows 2000 Server with the latest service pack
  - Windows Server 2003 (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 Mbits/s Ethernet link (1 Gbit/s 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 installing Symantec AntiVirus for Network Attached Storage on a Sun Solaris system:

**Operating system**

Solaris 9 and 10
Ensure that your operating system has the latest 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 Mbits/s Ethernet link (1 Gbit/s 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 installing Symantec AntiVirus for Network Attached Storage on a Linux system:

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 Mbits/s Ethernet link (1 Gbit/s 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.
  - 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\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.
  - 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.
Post-installation tasks

The Symantec AntiVirus for Network Attached Storage connectors do not require licensing from Symantec. However, you must install the appropriate licenses for Symantec Scan Engine. These licenses are required to activate antivirus scanning functionality for the scan engine and to receive updated virus definitions.

For more information about licensing, see the Symantec Scan Engine Implementation Guide.

After you install and configure the scan engine, you must configure the connector for your network attached storage device to send files to the scan engine.

For more information about integrating a specific connector with the scan engine, see the appropriate supported documentation provided by the manufacturer along with the NAS device documentation.

To access the latest supported network attached storage device documentation, see http://www.symantec.com/docs/TECH147442
A
antivirus scanning 13

B
Bloodhound 13

C
connector
  about 8, 10
container files 13

decomposer 13
denial-of-service attack 12
documentation
  Symantec AntiVirus for Network Attached Storage 11
  Symantec Scan Engine Implementation Guide 11

I
installation 14
installation requirements
  Linux 16
  Solaris 15
  Windows 14

L
Linux
  system requirements 16

M
malicious code 12

N
NAVEX 13

P
policy
  virus scan 7
polymorphic viruses 13

S
software components
  about 8
Solaris
  system requirements 15
Striker 13
Symantec antivirus technology
  Bloodhound 13
  examples 13
  NAVEX 13
  Striker 13
Symantec AntiVirus for Network Attached Storage
documentation 11
Integration Guide 11
Symantec Antivirus for Network Attached Storage
software components 8
Symantec Scan Engine
  about 8–9
documentation 11
protocols 9
virus protection 13
Symantec Scan Engine Implementation Guide
  about 11
Symantec Security Response
  about 13
  website 13

T
trojan horses 13

V
virus protection
  description 13
  for network attached storage 12
  why 12
virus scan policy 7
virus scanning
    add 8