Configuring Symantec AntiVirus™ for NetApp® Storage system™

Configuring Symantec™ AntiVirus for NetApp® Storage system™

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: 5.2.11

Legal Notice

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

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

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

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

Symantec Corporation
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

Configuring Symantec™ AntiVirus for NetApp® Storage system™

This document includes the following topics:

- About software components
- How Symantec Scan Engine works with the NetApp Storage system client
- About preparing for installation
- About configuring Symantec Scan Engine
- About configuring the client NetApp Storage system

About software components

Symantec AntiVirus for Network Attached Storage provides virus scanning and repair capabilities for Network Appliance™ (NetApp) Storage System™ storage appliances.

Configure the following components to add antivirus scanning to the NetApp Storage system:

- Symantec Scan Engine, which provides the virus scanning and repair services
  For more information, see the *Symantec Scan Engine Implementation Guide*.
- The NetApp Storage system
  Some options are configured directly on the NetApp Storage system. No additional code is necessary to connect Symantec Scan Engine to the NetApp

Storage system.See “About configuring the client NetApp Storage system” on page 26.

How Symantec Scan Engine works with the NetApp Storage system client

Symantec AntiVirus for Network Attached Storage provides virus scanning and repair capabilities for the NetApp Storage system storage appliances that support Data ONTAP™ version 8.0.2. Each Storage system must be running Data ONTAP 8.0.2 if you plan to use a single Symantec Scan Engine to support multiple Storage system storage appliances.

Symantec Scan Engine must be installed on a computer that is running Windows 2000 Server/Windows Server 2003/Windows Server 2008. Symantec Scan Engine 5.2.11 has been certified with Data ONTAP 8.0.2 for the following Windows Server platforms:

- Windows 2003 SP2 32-bit
- Windows 2008 SP2 64-bit
- Windows 2008 R2 SP1 64-bit

Symantec Scan Engine must be located in the same domain as the NetApp Storage system for which it provides scanning and repair services. This requirement does not apply if Symantec Scan Engine is installed on Windows Server 2003 with no patch. Symantec Scan Engine uses the proprietary Network Appliance adaptation of the RPC protocol to interface with NetApp Storage system storage appliances.

A single Symantec Scan Engine can support multiple NetApp Storage system. You can use multiple scan engines to support one or more Storage systems for sites with larger scan volumes. Load balancing is handled through the NetApp Storage system interface.

Virus scanning on the NetApp Storage system is available only for those files that are requested through the Common Internet File System (CIFS). Files that are requested through the Network File System (NFS) are not scanned for viruses.

What happens when a file is scanned

The NetApp Storage system submits files to Symantec Scan Engine for scanning on both read and write. That is, files are scanned when they are accessed from storage (read), renamed (write) and when submitted for storage, if modified (write).

When a user tries to access a file, the Storage system passes the file to Symantec Scan Engine for scanning. After a file is scanned, Symantec Scan Engine indicates the scanning results to the Storage system. If a file is infected and can be repaired, the scan engine returns the repaired file based on a configurable virus scan policy.

Clean files are passed to the requesting user after the Storage system receives the scanning results. The repaired file is passed to the requesting user if the file is infected and can be repaired. The stored version of the infected file is then replaced with the repaired file. The user is denied access to the file if the file is infected and cannot be repaired, and the infected file is deleted from storage. Symantec Scan Engine can be configured to quarantine these unrepairable files.

See “About quarantining unrepairable infected files” on page 20.

The Storage system caches scanning results for each clean file to avoid redundant scans of those files that have already been scanned. The cache is purged when the virus definitions on Symantec Scan Engine are updated, the “vscan reset” command is run on the Storage system, or when the scan engine is restarted. If the cache is full and a file that is not in the cache is accessed, the oldest information in the cache is purged. This ensures that the scanning results for the newly scanned file can be stored.

About connecting to Symantec Scan Engine

A connection is maintained between each NetApp Storage system and Symantec Scan Engine. Symantec Scan Engine monitors the connection with each NetApp Storage system by checking the connection at a configured time interval. The scan engine tries to reconnect if it determines that the connection is not active. (The number of times that the scan engine tries to re-establish the connection can also be configured.)

About limiting scanning by file type

Viruses are found only in the file types that contain executable code. Only those file types that can contain viruses need be scanned. Limiting scanning by file type saves bandwidth and time.

You have the following levels of control over which files are scanned:

You can control the files that are initially submitted to the scan engine by the NetApp Storage system for scanning	The NetApp Storage system lets you specify by file extension the files that are to be passed to Symantec Scan Engine for scanning. You configure the file types that you want to submit for scanning through the NetApp Storage system interface in accordance with the product documentation. See "About specifying the file extensions to be scanned on the NetApp Storage system" on page 27.
You can control the files that are embedded in archival file formats (for example, .zip or .lzh files) that are to be scanned by Symantec Scan Engine	The scan engine lets you specify the file types and the file extensions that you do not want to scan. The file extensions exclusion list and the file type exclusion list achieve this purpose. You can also scan all file types regardless of extension. You configure which embedded files are scanned through the Symantec Scan Engine administrative interface. See "Specify which embedded files to scan" on page 21.

About handling infected files

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

Scan Only	Deny access to the infected file, but do nothing to the infected file.
Scan and repair files	Try to repair the infected file, and deny access to any unrepairable file.
Scan and repair or delete	Try to repair the infected file, and delete any unrepairable file.

You can also configure the scan engine to quarantine unrepairable files.

See "About quarantining unrepairable infected files" on page 20.

About user identification and notification when a virus is found

When a virus is found in a file that is requested from the NetApp Storage system, Symantec Scan Engine automatically obtains (for logging purposes) identification information about the user who requested the infected file. This information includes the security identifier of the user and the IP address and host name of the requesting computer.

The identification information supplements the information that is contained in Infection Found log messages that are logged to the local logs, the Windows Event Log, and SMTP. This information does not appear in the Infection Found messages that are logged to SNMP or SESA.

Note: Symantec Scan Engine can obtain only the information that is made available by the NetApp Storage system. In some cases, all or some of this information is not available. The information that is obtained is reported in the related log entries. Any identification information that is not obtained from the NetApp Storage system 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 virus was found.The notification message includes the following:

- Date and time of the event
- File name of the infected file
- Virus name and ID
- Virus definition date and revision number
- Manner in which the infected file was handled (for example, the file was repaired or deleted)
- Scan policy
- Disposition of the file
- Duration of scan time and connection time

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

See "Notifying a requesting user that a virus was found" on page 18.

About preparing for installation

The NetApp Storage System storage appliance must support Data ONTAP version 8.0.2 to interface with Symantec Scan Engine. If you plan to use a single Symantec Scan Engine to support multiple Storage system storage appliances, each Storage system must support Data ONTAP version 8.0.2. As a prerequisite, ensure that each NetApp Storage System for which the scan engine is to provide scanning and repair services meets this requirement.

To use RPC, Symantec Scan Engine must be installed on a computer that is running Windows 2003 SP2 32-bit/Windows 2008 SP2 64-bit/Windows 2008 R2 SP1 64-bit. The computer on which you plan to install Symantec Scan Engine must meet the system requirements that are listed in the Symantec Scan Engine Implementation Guide.

After you install Symantec Scan Engine, configure the NetApp Storage System to work with the scan engine.

See "About configuring the client NetApp Storage system" on page 26.

About configuring Symantec Scan Engine

Configure Symantec Scan Engine to use RPC as the communication protocol. The Internet Content Adaptation Protocol (ICAP) is the default protocol at installation, but you can change the protocol to RPC through the administrative interface. Then you can configure the RPC-specific options.

See "Configuring RPC protocol options" on page 14.

You must also change the Windows service startup properties to identify an account that has the appropriate permissions.

See "Editing the service startup properties" on page 12.

Editing the service startup properties

If you change the protocol setting to RPC, you need to change the service startup properties to identify an account that has the following appropriate permissions:

- The user account must have local administrator permissions on the computer that has the scan engine.
- The user account must have Backup Operator privileges or above on the NetApp Storage system.

You must change the service startup properties if the list of NetApp Storage systems is edited as well.

To edit the service startup properties

1. In the Windows 2003 SP2 32-bit/Windows 2008 SP2 64-bit/Windows 2008 R2 SP1 64-bit 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 user account that has local administrator rights on the computer that has the scan engine. This account should also have domain backup operator privileges or above.

   Use the following format for the account name:

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

   For more information on stopping and starting the Symantec Scan Engine service, see the *Symantec Scan Engine Implementation Guide*.

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-inHTTPS 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 an HTTP server.

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

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.

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.

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**.

Configuring RPC protocol options

After you install Symantec Scan Engine, you can configure settings that are specific to the RPC protocol. You must manually stop and start the scan engine service when you change to the RPC protocol. A proper connection to the NetApp Storage system is ensured.

Table 1-1 describes the protocol-specific options for RPC.

Table 1-1 Protocol-specific options for RPC

Option	Description
RPC client list	A single Symantec Scan Engine can support one or more NetApp Storage systems. NetApp Storage systems must be located in the same domain as the scan engine. You must provide the IP address of each NetApp Storage system. **Note:** Multiple scan engines can support a single NetApp Storage system. Configure the multiple scan engines through the NetApp Storage system interface.

Table 1-1 Protocol-specific options for RPC *(continued)*

Option	Description
Check RPC connection every __ seconds	Symantec Scan Engine maintains a connection with the NetApp Storage system. Symantec Scan Engine can be configured to check the connection with the NetApp Storage system at a prescribed interval to ensure that the connection is active. The default value is 20 seconds.
Maximum number of reconnect attempts	You can configure the scan engine to make a specified number of tries to re-establish a lost connection with the NetApp Storage system. By default, Symantec Scan Engine is configured to try to reconnect with the NetApp Storage system indefinitely. **Note:** Do not set a maximum number of reconnect attempts if the scan engine provides scanning for multiple NetApp Storage systems. Use the default setting.
Antivirus scan policy	You can configure Symantec Scan Engine to do one of the following when an infected file is found: ■ Scan only: Deny access to the infected file, but do nothing to the infected file. ■ Scan and repair files: Try to repair the infected file, and deny access to any unrepairable file. ■ Scan and repair or delete: Try to repair the infected file, and delete any unrepairable file from archive files. **Note:** You must select Scan and repair or delete if you plan to quarantine the infected files that cannot be repaired. For more information, see the Symantec Scan Engine Implementation Guide.
Automatically send antivirus update notifications	You can configure Symantec Scan Engine to automatically notify the NetApp Storage system when new virus definitions are used. This notification causes the NetApp Storage system to clear its cache of scanned files.

Configure RPC protocol options

To configure RPC, do the following:

- Provide an IP address for each NetApp Storage system for which Symantec Scan Engine should provide scanning services. You can add or delete Storage systems from this list at any time.
- Configure the additional RPC-specific options.

To edit the list of NetApp Storage system

1. On the Symantec Scan Engine administrative interface, in the left pane, click **Configuration**.
2. Under Views, click **Protocol**.
3. In the right pane, under Select Communication Protocol, click **RPC**.

   The configuration settings are displayed for the selected protocol.
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 administrative interface. However, the changes do not take effect until you restart the Symantec Scan Engine service.
5. To add a NetApp Storage system to the list of RPC clients, type the IP address of the NetApp Storage system for which Symantec Scan Engine should provide scanning services. Type one entry per line.
6. To delete a NetApp Storage system from the list of RPC clients, select and delete the IP address of the NetApp Storage system.
7. On the toolbar, select one of the following:

Save	Saves your changes. You can continue to make changes in the administrative interface until you are ready to apply them.
Apply	Applies your changes. Your changes are not implemented until you apply them. You must perform a manual restart for the changes to take place and for a proper connection to the NetApp Storage system.

To configure additional RPC-specific options

1. On the Symantec Scan Engine administrative interface, in the left pane, click **Configuration**.
2. Under Views, click **Protocol**.
3. Under RPC Configuration, in the Check RPC connection every box, type how frequently Symantec Scan Engine checks the RPC connection with the NetApp Storage system 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 tries that the Symantec Scan Engine should undertake to reestablish a lost connection with the NetApp Storage system.

The default setting is 0. Symantec Scan Engine tries indefinitely to reestablish a connection. Use the default setting if the scan engine provides scanning for multiple NetApp Storage systems.

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

The default setting is Scan and repair or delete.

6 On the toolbar, select one of the following:

Save	Saves your changes. You can continue to make changes in the administrative interface until you are ready to apply them.
Apply	Applies your changes. Your changes are not implemented until you apply them. You must perform a manual restart for the changes to take place and for a proper connection to the NetApp Storage system.

Notifying the NetApp Storage system when virus definitions are updated

When Symantec Scan Engine scans a file, it is stored in the NetApp Storage system's cache. This cached file is sent to any user who subsequently requests the same file thus conserving scanning resources.

You can configure the scan engine to automatically notify the NetApp Storage system when the scan engine begins using new virus definitions. This notification prompts the NetApp Storage system to clear its cache of scanned files. Any new requests for files causes the file to be sent to the scan engine again for scanning. The scanned clean files are cached, and these cached files are sent to the requesting user.

You can manually clear the cache of scanned files at the command line interface of the NetApp Storage system as well.

See "About clearing the scanned files cache" on page 29.

The process of automatically notifying the NetApp Storage system about virus definitions updates could affect system performance, depending on how frequently you schedule LiveUpdate. You can send the notification manually to minimize the impact on scanning resources.

To automatically notify the NetApp Storage system when virus definitions are updated

1 On the administrative interface, in the left pane, click **Configuration**.

2 Under Views, click **Protocol**.

3 Under RPC Configuration, check Automatically send AntiVirus update notifications.

This option is disabled by default.

4 On the toolbar, select one of the following:

Save	Saves your changes. You can continue to make changes in the administrative interface until you are ready to apply them.
Apply	Applies your changes. Your changes are not implemented until you apply them. You must perform a manual restart for the changes to take place.

To manually notify the NetApp Storage system when virus definitions are updated

1 On the administrative interface, in the left pane, click **Configuration**.

2 Under Views, click **Protocol**.

3 In the left pane, under Tasks, click **Send AntiVirus Update Notification**.

Notifying a requesting user that a virus was found

You can configure Symantec Scan Engine to notify the requesting user that the retrieval of a file failed because a virus was found. The notification message is displayed only if the user uses a Windows computer. In addition, the requesting user's computer must be in the same domain as the scan engine. Both the user's computer and the scan engine must have the Windows Messenger service running to use this feature.

The notification message includes the following information:

- The date and time of the event
- The event security level (for example, Warning)
- The scan policy (for example, scan and repair or delete)
- The file name of the infected file
- The virus name and ID
- The manner in which the infected file was handled (for example, the file was repaired or deleted)
- The disposition of the file (for example, infected)
- The IP address and name of the requesting user's computer
- The date and revision number of the virus definitions used
- The duration (in seconds) of scan and connection time

You can enable the NetApp Storage system to display warning messages to the requestinguser as well.

See "About notifying a requesting user that a virus was found" on page 29.

To notify a requesting user that a virus was found

1. On the Symantec Scan Engine administrative interface, in the left pane, click **Monitors**.
2. Under Views, click **Alerting**.
3. In the right pane, under Log Windows Messenger, check **Enable Windows Messenger Logging**.

   User notification is disabled by default.
4. On the toolbar, select one of the following:

Save	Saves your changes. You can continue to make changes in the administrative interface until you are ready to apply them.
Apply	Applies your changes. Your changes are not implemented until you apply them. You must perform a manual restart for the changes to take place.

About quarantining unrepairable infected files

You can quarantine unrepairable infected files when you use the RPC protocol. To achieve the quarantine feature, Symantec Central Quarantine must be installed separately on a computer that runs Windows 2000 Server/Windows 2003 Server. Symantec Central Quarantine is included on the Symantec Scan Engine distribution CD along with supporting documentation.

Symantec Scan Engine forwards the infected files that cannot be repaired to Symantec Central Quarantine. Typically, the heuristically-detected viruses that cannot be eliminated by the current set of virus definitions are forwarded to the quarantine. They are isolated so that the viruses cannot spread. The infected items can be submitted to Symantec Security Response for analysis from the quarantine. New virus definitions are posted if a new virus is identified.

Note: You must select “Scan and repair or delete” as the RPC scan policy to forward files to the quarantine. The original infected file is deleted when a copy of an infected file is forwarded to the quarantine. If submission to the quarantine is not successful, the original file is not deleted, and an error message is returned to the NetApp Storage system. Access to the infected file is denied.

For more information about installing and configuring Symantec Central Quarantine, see the *Symantec Central Quarantine Administrator’s Guide*.

To quarantine unrepairable infected files

1. On the Symantec Scan Engine administrative interface, in the left pane, click **Policies**.
2. Under Views, click **Scanning**.
3. In the right pane, 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 is installed.

5 In the Port box, type the TCP/IP port number to be used by the Symantec Scan Engine to pass files to the Symantec Central Quarantine.

This setting must match the port number that is selected at installation for Symantec Central Quarantine.

6 On the toolbar, select one of the following:

Save	Saves your changes. You can continue to make changes in the administrative interface until you are ready to apply them.
Apply	Applies your changes. Your changes are not implemented until you apply them.

Specifying which embedded files to scan

The NetApp Storage system submits files to Symantec Scan Engine for scanning based on the file extension of the top-level file. You can configure the file types that are submitted for scanning through the Storage system administrative interface. The top-level files that are sent to Symantec Scan Engine are scanned regardless of file extension.

When the scan engine receives an archive file (for example, a .zip or .lzh file) that contains embedded files, it must break down the archive file and scan each embedded file. You can control, through the scan engine administrative interface, which embedded files are scanned by using a file extension and file type exclusion list. You can also scan all files regardless of extension.

Symantec Scan Engine is configured by default to scan all files. The file type and file extension exclusion list is prepopulated with the file types that are unlikely to contain viruses, but you can edit this list.

Note: During virus outbreaks, you might want to scan all files even if you normally control the file types that are scanned with the file type or file extension exclusion list.

Specify which embedded files to scan

You can scan all files regardless of extension, or you can control which files are scanned by specifying the extensions or the file types that you want to exclude. Symantec Scan Engine is configured by default to scan all files.

To scan all files regardless of extension or type

1. On the Symantec Scan Engine administrative interface, in the left pane, click **Policies**.
2. Under Views, click **Scanning**.
3. In the right pane, under Files to Scan, click **Scan all files**.
4. On the toolbar, select one of the following:

Save	Saves your changes. You can continue to make changes in the administrative interface until you are ready to apply them.
Apply	Applies your changes. Your changes are not implemented until you apply them.

To scan all files except for those that are in the file extension exclusion list

1. On the Symantec Scan Engine administrative interface, in the left pane, click **Policies**.
2. Under Views, click **Scanning**.
3. In the right pane, under Files to Scan, click **Scan all files except those in the extension or type exclude lists**.

   On activating this option, both the file extension exclude list and the file type exclude list gets activated automatically.
4. Type each file extension that you want to add to the list on a separate line.

   Use a period with each extension in the list.
5. To remove a file extension from the list, select it and delete it from the File extension exclude list.

6 To restore the default file extension exclude list, in the left pane, under Tasks, click **Reset Default List**.

This option restores the default file-type exclude list and the file-extension exclude list.

7 On the toolbar, select one of the following:

Save	Saves your changes. You can continue to make changes in the administrative interface until you are ready to apply them.
Apply	Applies your changes. Your changes are not implemented until you apply them.

To scan all file types except those in the file type exclusion list

1 On the Symantec Scan Engine administrative interface, in the left pane, click **Policies**.

2 Under Views, click **Scanning**.

3 In the right pane, under Files to Scan, click **Scan all files except those in the extension or type exclude lists**.

When you activate this option, both the file type exclude list and the file extension exclude list are activated automatically.

4 Type each file type you want to add to the list on a separate line.

To include all subtypes for a file type, use the wildcard character /*.

5 To remove a file type from the list, select it and delete it from the File type exclude list.

6 To restore the default file type exclude list, in the left pane, under Tasks, click **Reset Default List**.

This option restores the default file-type exclude list and the file-extension exclude list.

7 On the toolbar, select one of the following:

Save	Saves your changes. You can continue to make changes in the administrative interface until you are ready to apply them.
Apply	Applies your changes. Your changes are not implemented until you apply them.

Scheduling LiveUpdate to update virus definitions automatically

Scheduling LiveUpdate to occur automatically at a specified time interval ensures that the Symantec Scan Engine always has the most current virus definitions. If you use multiple scan engines to support virus scanning, schedule LiveUpdate to occur at the same time for each scan engine. This scheduling ensures that all scan engines have the same version of virus definitions. Having the same version of virus definitions is necessary for proper functioning of virus scanning on the NetApp Storage system.

You must schedule LiveUpdate on each Symantec Scan Engine. When LiveUpdate is scheduled, LiveUpdate runs at the specified time interval relative to the LiveUpdate base time. The default LiveUpdate base time is the time that the scan engine was installed.

You can change the LiveUpdate base time. If you change the scheduled LiveUpdate interval, the interval adjusts based on the LiveUpdate base time.

For more information on changing the base time, see the *Symantec Scan Engine Implementation Guide*.

To schedule LiveUpdate to update virus definitions automatically

1 On the Symantec Scan Engine administrative interface, in the left pane, click **System**.

2 Under Views, click **LiveUpdate Content**.

3 In the right pane, under LiveUpdate Content, check **Enable scheduled LiveUpdate**.

This option is enabled by default.

4 In the LiveUpdate interval drop-down list, choose an interval.

You can select from 2, 4, 8, 10, 12, or 24-hour intervals. The default LiveUpdate interval is 2 hours.

5 On the toolbar, select one of the following:

Save	Saves your changes. You can continue to make changes in the administrative interface until you are ready to apply them.
Apply	Applies your changes. Your changes are not implemented until you apply them.

Configuring Rapid Release updates to occur automatically

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.

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.

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.

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.

Configuring Rapid Release updates to occur automatically

1. On the Symantec Scan Engine administrative interface, in the left pane, click **System**.
2. 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:

Save	Saves your changes. You can continue to make changes in the administrative interface until you are ready to apply them.
Apply	Applies your changes. Your changes are not implemented until you apply them.

About configuring the client NetApp Storage system

After you configure Symantec Scan Engine to use RPC as the communication protocol, you configure the client NetApp Storage systems to work with Symantec Scan Engine.

NetApp Storage system clients must be running Data ONTAP version 8.0.2 to interface with Symantec Scan Engine. If you plan to support more than one Storage system with a single scan engine, each Storage system must be running Data ONTAP 8.0.2.

Each NetApp Storage system should be installed and configured in accordance with the accompanying product documentation. Each Storage system should be functional before you initiate virus scanning using Symantec Scan Engine.

About verifying that the scan engine is registered with the Storage system

You can verify that the scan engine is registered with the Storage system after you install Symantec Scan Engine. Registration is automatic if you have provided the correct information to Symantec Scan Engine for contacting the Storage system. Registration occurs when the scan engine connects to the Storage system. Use the “vscan” command at the command line interface to check the list of registered scan engines.

Note: The service startup properties for Symantec Scan Engine must be changed to identify an account that has the appropriate permissions on the Storage system. If the change has not been done, the scan engine cannot register with the Storage system because it does not have sufficient permission.

See “Editing the service startup properties” on page 12.

About activating virus scanning

You can activate and deactivate virus scanning. Use the “vscan on” command at the command line to activate virus scanning. Use the “vscan off” command to deactivate virus scanning.

About specifying the file extensions to be scanned on the NetApp Storage system

Configure the list of extensions on the NetApp Storage system to contain only the file extensions that you want to scan. This lets you control the file types that are passed to Symantec Scan Engine for scanning. You can configure file extensions using the extensions include and exclude list. The extensions that are configured on the NetApp Storage system have preference over the file types and the extensions configured on Symantec Scan Engine. For example, if .doc is included in the extensions include list for the NetApp Storage system but is excluded on Symantec Scan Engine, .doc files are still scanned.

A default list of extensions to be submitted for virus scanning is included with the NetApp Storage system. To modify the extensions include list, at the command line interface, use the “vscan extensions include add” command to add additional extensions and the “vscan extensions include remove” command to remove extensions from the list.

Similarly, for the extensions exclude list, the “vscan extensions exclude add” command would add extensions to the exclude list while the “vscan extensions exclude remove” would successfully remove extensions from the exclude list on the NetApp Storage system.

To rollback to the default include list, use the “vscan extensions include reset” command at the command line interface. The wildcard extension (???), which scans all files regardless of file extension, might negatively impact performance. The highest level of protection is achieved by scanning all file types; however, viruses are found only in those file types that contain executable code. So, every file type need not be scanned. You can save bandwidth and time by limiting the files to be scanned to only those file types that can contain viruses.

For more information, see the NetApp Storage system documentation.

About working with unresponsive scan engines

The NetApp Storage system can be configured to let the connection time out while waiting for a reply from Symantec Scan Engine. Connections mostly time out when large or complex files are scanned (for example, container files with multiple embedded files or files that contain polymorphic or macro viruses). The time out option can be configured by using the “vscan options time-out” command. The default value is 10 seconds. When the scan request times out, the NetApp Storage system Enable Windows Messenger Loggings to see if the scan engine is currently at work on its request. If there is still no response, it sends the scan request to another scan engine.

If none of the scan engines respond, then the NetApp Storage system can either allow file access without virus scanning or deny file access altogether. Configure this option by using the “vscan options mandatory_scan” command.

You can end a virus scanning session by the “vscan scanners stop” command.

For more information, see the NetApp Storage system documentation.

How virus scanning affects backups on NetApp Storage system

The service startup properties for Symantec Scan Engine must be edited to identify an account with Backup Operator privileges on the NetApp Storage system. Otherwise, backups on the Storage system might not finish successfully when virus scanning is active.

The NetApp Storage system can time out while waiting for a reply from the Symantec Scan Engine when large files are scanned. Virus scanning also increases the length of time that is needed for a backup to finish.

Note: Ensure that you have edited the service startup privileges appropriately, or disable virus scanning before you initiate a backup of the NetApp Storage system.

See “Editing the service startup properties” on page 12.

About clearing the scanned files cache

When Symantec Scan Engine scans a file, it is stored in the NetApp Storage system’s cache. This cached file is sent to any user who subsequently requests the same file thus conserving scanning resources. Symantec Scan Engine can automatically notify the NetApp Storage system when the scan engine begins using new virus definitions. This notification prompts the NetApp Storage system to clear its cache of scanned files. Any new requests for files causes the file to be sent to the scan engine again for scanning.

See “Notifying the NetApp Storage system when virus definitions are updated” on page 17.

You can manually clear the cache of scanned files by using the “vscan reset” command at the command line interface.

About notifying a requesting user that a virus was found

You can configure Symantec Scan Engine to notify the requesting user that the retrieval of a file failed because a virus was found.

See “Notifying a requesting user that a virus was found” on page 18.

You can also enable Data ONTAP on the NetApp Storage system to display warning messages by the “vscan options client_msgbox {on|off}” command.

Index

A

antivirus scan policy
- configure 15
- RPC option 14
- scan and repair files 14
- scan and repair or delete 14
- scan only 14

C

CIFS 8
Common Internet File System 8

D

Data ONTAP 8, 11

E

enable Windows messenger logging 18
event security level 18

F

file extension exclusion list 21
file type exclusion list 21
file types to be scanned
- NetApp Storage system 21

I

ICAP
- default protocol 12

infected file 14
infected files 10
Internet Content Adaptation Protocol 12

N

NetApp Storage System
- system requirements 11

NetApp Storage system
- activate virus scanning 27
- adding Symantec AntiVirus 7
- backups 28

NetApp Storage system *(continued)*
- cache 17, 29
- configure 26
- configuring for virus scanning 26
- Data ONTAP 8
- edit list 15
- editing service startup properties 12
- overview of virus scanning 8
- protocol 8
- quarantining infected files 20
- rollback 27
- software components 7
- specify file extensions 27
- user notification of infection found 18
- verify scan engine registration 27
- vscan extensions exclude add 27
- vscan extensions exclude remove 27
- vscan extensions include add 27
- vscan extensions include remove 27
- vscan extensions include reset 27

NetApp Storage system:specifying files to scan 21
Network Appliance Storage system 7
Network File System 8
NFS 8
notification message
- information contained 18
- virus name 18

notification of infection found
- NetApp Storage system 18

P

Preparing for installation 11

Q

quarantine
- irreparable file 8, 20
- procedure 20
- RPC scan policy 20
- unrepairable file 10

quarantining infected files
- NetApp Storage system 20

R

RPC
- client list 14
- configure 14
- handling infected files 10
- reconnect attempts 14

RPC client list 14

RPC protocol
- NetApp Storage system 8
- options 14

S

scan policy
- notification message 18

service startup properties
- edit for RPC 12
- NetApp Storage system 12

software components
- NetApp Storage system 7

Symantec Central Quarantine 20

Symantec Scan Engine
- administrative interface 12
- change protocol 12
- configure 12
- configuring for NetApp Storage system 12
- quarantine 8
- Rapid Release 25
- scan all files 21

Symantec Security Response
- infected files 20

U

unrepairable files 10

unrepairable infected file 20

unresponsive scan engines 28

V

virus
- heuristically detected 20
- notification 10
- user identification 10

virus definition
- automatic notification 17
- automatic update 24
- new 20
- on updating 17
- Rapid Release definitions 25

vscan 27

vscan off 27

vscan on 27

vscan options mandatory_scan 28

vscan options timeout 28

vscan reset 8

W

wildcard extension
- ??? 27

Windows messenger service 18

Windows service startup properties 12