Configuring Symantec™ Protection Engine for Network Attached Storage 7.8 for NetApp® Data ONTAP®
Configuring Symantec™ Protection Engine for Network Attached Storage 7.8 for NetApp® Data ONTAP®.

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.

Legal Notice

Copyright © 2017 Symantec Corporation. All rights reserved.

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

This Symantec product may contain third party software for which Symantec is required to provide attribution to the third party (“Third Party Programs”). Some of the Third Party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. Please see the Third Party 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 website 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:


**Customer service**

Customer service information is available at the following URL:


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

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

**Support agreement resources**

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

Asia-Pacific and Japan  
[customercare_apac@symantec.com](mailto:customercare_apac@symantec.com)

Europe, Middle-East, and Africa  
[semea@symantec.com](mailto:semea@symantec.com)

North America and Latin America  
[supportsolutions@symantec.com](mailto:supportsolutions@symantec.com)
Installing and configuring Symantec™ Protection Engine for Network Attached Storage 7.8

This chapter includes the following topics:

- Before you install Symantec Protection Engine
- System requirements to install Symantec Protection Engine on Windows
- About installing Symantec Protection Engine
- Installing Symantec Protection Engine on Windows
- Editing the service start-up properties
- Configure LiveUpdate to occur automatically
- Configuring Rapid Release updates to occur automatically
- About connecting to Symantec Protection Engine

Before you install Symantec Protection Engine

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

See "System requirements to install Symantec Protection Engine on Windows"

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

- Disable any third-party antivirus products that are running on the server on which you plan to install Symantec Protection Engine. You can turn on antivirus protection after installation is complete. Symantec Protection Engine scans the files that client applications pass to Symantec Protection Engine. Symantec
Protection Engine does not protect the computer on which it runs. Since Symantec Protection Engine processes the files that might contain threats, the server on which it runs is vulnerable if it has no real-time protection. Use an antivirus program to protect the server on which Symantec Protection Engine runs, such as Symantec Endpoint Protection. To prevent scanning conflicts, configure the antivirus program not to scan the temporary directory that Symantec Protection Engine uses for scanning.

- Review the deployment considerations and recommendations. These recommendations can enhance your overall performance. For more information, please refer to the Symantec™ Protection Engine for Network Attached Storage Implementation Guide included in product zip file.

**System requirements to install Symantec Protection Engine on Windows**

Before you install Symantec Protection Engine, verify that your server meets the minimum system requirements. The minimum system requirements to install Symantec Protection Engine on Windows are as follows:

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

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

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

Memory
- 8 GB RAM or higher

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

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

Hypervisor support
- Windows 2008 R2 Hyper-V
- Windows 2012 Hyper-V
- VMware® vSphere 5.5 or later
- VMware® vSphere 6.0 or later

The following Windows guest operating systems have been certified on Hyper-V:
- Windows Server 2008 SP2 (64-bit)
- Windows Server 2008 R2 (64-bit)
About installing Symantec Protection Engine

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

**Installer check results** describes the action taken by the installer when no previous version is installed or an existing version of Symantec Protection Engine is installed.

<table>
<thead>
<tr>
<th>Table 2-1</th>
<th>Installer check results</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Version</strong></td>
<td><strong>Action taken by installer</strong></td>
</tr>
<tr>
<td>No previous version is detected</td>
<td>A full installation is performed</td>
</tr>
<tr>
<td>7.5.x is already installed on the computer</td>
<td>A separate utility to migrate from 7.5.x to 7.8 will be provided. For more information, see the Symantec Protection Engine 7.8 Migration Utility at the following location: <a href="https://support.symantec.com/en_US/article.INFO3603.html">https://support.symantec.com/en_US/article.INFO3603.html</a></td>
</tr>
<tr>
<td>Version 7.0.x is detected</td>
<td>Symantec Protection Engine 7.8 does not support upgrades from version 7.0.x. You must first upgrade to version 7.5.x and then use migration utility mentioned above to migrate to version 7.8.</td>
</tr>
<tr>
<td>Version 5.1 or 5.2 is detected</td>
<td>Symantec Protection Engine does not support direct upgrades from version 5.1/5.2. You must first upgrade to version 7.0.x, then upgrade to version 7.5.x, and then use migration utility mentioned above to migrate to version 7.8.</td>
</tr>
</tbody>
</table>

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

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

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

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

For more information, see the Symantec™ Protection Engine for Network Attached Storage Implementation Guide included in the product zip file.
Installing Symantec Protection Engine on Windows

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

See "System requirements to install Symantec Protection Engine on Windows"

**Note:** Symantec recommends that you install Symantec Protection Engine with Administrative or equivalent privilege account. Also, for security purposes, the read, write, and execute permissions for all Symantec Protection Engine-based files should be denied for all other users.

When the installation is complete, Symantec Protection Engine is installed as a Windows 2008/2012 service. It is listed as Symantec Protection Engine in the Services Console. The Symantec Protection Engine service starts automatically when the installation is complete. Any significant installation activities are recorded in the Windows Application Event Log.

**To install Symantec Protection Engine on Windows**

1. Log on to the computer on which you plan to install Symantec Protection Engine as administrator or as a user with administrator rights.
2. In the Symantec Protection Engine.zip file, run SymantecProtectionEngine.exe.
3. In the Welcome panel, click Next.
4. In the License Agreement panel, after you read the agreement, indicate that you agree with the terms of the Symantec Software License Agreement, and then click Next.
   The default setting is that you do not agree with the terms of the Symantec Software License Agreement. If you do not indicate that you agree, the installation is canceled.
5. In the Deployment Scenario panel, select the type of deployment that Symantec Protection Engine should protect.
   If you select Other Application, enter the name of the application in the provided field.
   Note: The maximum length of the application name can be up to 40 characters.
6. In the Destination Folder panel, select the location to install Symantec Protection Engine, and then click Next.
   The default location is C:\Program Files\Symantec\Scan Engine for Windows platform.
   Note: If you plan to change the default location to install Symantec Protection Engine, make sure the new directory has the same permissions as that of the Program Files Directory.
   Warning: If the new location to install Symantec Protection Engine does not have the same permissions as that of the Program Files directory, malicious users with lower privilege can read and copy file contents, replace malicious data in tags, rename the file, or even delete the product files.
7. In the URL filtering panel, select the provided option to enable URL filtering feature and downloading of URL definitions.
8. In the Reputation-based Protection (Insight) panel, select the Enable Insight check box to enable the Insight feature.
   The Select Insight Aggression Level drop-down list is enabled only if you select the Enable Insight check box.
9. Select the Insight aggression level.
   The Insight aggression level defines how sensitive the Symantec Insight™ feature is to a file's reputation score.
10. In the Ready to Install the Program panel, click Install.
11. Click Finish.

**Editing the service start-up properties**

If you change the protocol setting to RPC, you need to change the service start-up 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 protection engine.
- The user account must have Backup Operator privileges or above on the NetApp storage system.

You must change the service start-up properties if the list of NetApp storage systems is edited as well.

**To edit the service startup properties**

1. On the Windows Server 2008 SP2 (64-bit) or Windows Server 2008 R2 SP1 (64-bit) or Windows Server 2012 (64-bit) Control Panel, click Administrative Tools.
2. Click Services.
3. In the list of services, right click Symantec Protection Engine, and then click Properties.
4. In the Properties dialog box, on the Log On tab, click This Account.
5. Type the account name and password for the user account that has local administrator rights on the computer that has Symantec Protection Engine installed. 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 restart the Symantec Protection Engine service. For more information on stopping and restarting the Symantec Protection Engine service, see the Symantec™ Protection Engine for Network Attached Storage Implementation Guide.

**To edit the list of NetApp storage systems**

1. Go to Symantec Protection Engine installation directory.
2. Execute the following XMLmodifier commands:
   - To change protocol to RPC:
     XMLModifier.exe -s /configuration/ProtocolSettings/Protocol/@value RPC configuration.xml
   - To add a NetApp storage system to the list of RPC clients:
     XMLModifier.exe -s /configuration/ProtocolSettings/RPC/ClientList/items/item/@value 127.0.0.1 configuration.xml
   - To remove the RPC client:
     XMLModifier.exe -r /configuration/ProtocolSettings/RPC/ClientList/items/item/@value configuration.xml
3. Restart Symantec Protection Engine service.

**To configure additional RPC-specific options**

1. Go to Symantec Protection Engine installation directory.
2. To check how frequently Symantec Protection Engine should check the RPC connection with the NetApp storage system to ensure that the connection is active use following command:

```
XMLModifier.exe -s/configuration/ProtocolSettings/RPC/RPCConnectionCheckInterval/@value <value> configuration.xml
```

Replace the `<value>` with desired value. For example, 30.

3. To check maximum number of tries that the Symantec Protection Engine should undertake to re-establish a lost connection with the NetApp storage system use following command. The default setting is 0. Symantec Protection Engine tries indefinitely to re-establish a connection.

```
XMLModifier.exe -s/configuration/ProtocolSettings/RPC/RPCMaxReconnectAttempts/@value <value> configuration.xml
```

Replace the `<value>` with desire value.

4. Restart Symantec Protection Engine service.

**To configure the antivirus scan policy**

1. Go to Symantec Protection Engine installation directory.

2. To change AV Action policy, execute the following command:

```
XMLModifier.exe -s/policies/ThreatPolicies/Actions/AVActionPolicy/@value <value> policy.xml
```

Where `<value>` can be

- 0 - Which is Scan Only
- 1 - Scan and Repair Files
- 2 - Scan and Repair or delete

3. Restart Symantec Protection Engine service.

The description of the values are as follows:

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

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

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

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

You can schedule LiveUpdate to occur automatically at a specified time interval to ensure that Symantec Protection Engine always has the most current definitions. When you install a valid antivirus content license or URL content license, Symantec Protection Engine automatically tries to perform a LiveUpdate. By default, Symantec Protection Engine is configured to perform a LiveUpdate every two hours.

When LiveUpdate is scheduled, it runs at the specified time interval that is relative to the LiveUpdate base time. The default LiveUpdate base time is the time that Symantec Protection Engine was installed. You can change the LiveUpdate base time by editing the configuration file. If you change the scheduled LiveUpdate interval, the interval adjusts based on the LiveUpdate base time.

To configure LiveUpdate to occur automatically

1. Go to the Symantec Protection Engine installation directory.
2. Enable LiveUpdate schedule using the following command:
   `xmlmodifier -s //liveupdate/Schedule/@enabled true liveupdate.xml`

   **Allowed values:**
   - True: Enables LiveUpdate.
   - False: Disables LiveUpdate.

   **Default value:** true
3. In the LiveUpdate interval list, select the interval.

   **Command:**
   `xmlmodifier -s //liveupdate/Schedule/Interval/@value <value> liveupdate.xml`

   **Allowed values:** Any numerical value in seconds.

   **Default value:** 7200

Configuring Rapid Release updates to occur automatically

You can configure Symantec Protection Engine to obtain uncertified definition updates with Rapid Release. You can configure Symantec Protection Engine to retrieve Rapid Release definitions every 5 to 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 in 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 Protection Engine always has the most current definitions. Scheduled Rapid Release updates are disabled by default.
Configuring Rapid Release updates to occur automatically

1. Go to the Symantec Protection Engine installation directory.
2. Configure Rapid Release updates to occur automatically.
   
   **Command:**
   
   `xmlmodifier -s //liveupdate/RapidRelease/Schedule/@enabled true liveupdate.xml`
   
   **Allowed values:**
   
   - True: Enables Rapid Release updates.
   - False: Disables Rapid Release updates.
   
   **Default value:** false

3. In the Rapid Release interval specify the interval between which you want Symantec Protection Engine to download Rapid Release definitions.
   
   **Command:**
   
   `xmlmodifier -s //liveupdate/RapidRelease/Schedule/Interval/@value <value> liveupdate.xml`
   
   **Allowed values:** You can select any number between 5 minutes and 120 minutes.
   
   **Default value:** 30

4. Restart Symantec Protection Engine service.

About connecting to Symantec Protection Engine

A connection is maintained between each NetApp storage system and Symantec Protection Engine. Symantec Protection Engine monitors the connection with each storage system by checking the connection at a configured time interval. The protection engine tries to reconnect if it determines that the connection is not active. The number of times that the protection engine tries to re-establish the connection can also be configured.
Configuring Symantec™ Protection Engine for Network Attached Storage 7.8 for NetApp® Data ONTAP® operating in 7-Mode

This chapter includes the following topics:

- About software components for NetApp® Data ONTAP® when operating in 7-Mode
- How Symantec Protection Engine works with the NetApp storage system operating in 7-Mode
- What happens when a file is scanned when operating in 7-Mode
- About limiting scanning by file type when operating in 7-Mode
- About handling infected files when operating in 7-Mode
- About user identification and notification when a virus is found when operating in 7-Mode
- About preparing for installation when operating in 7-Mode
- About configuring Symantec Protection Engine to work with NetApp operating in 7-Mode
- Notifying the NetApp storage system operating in 7-Mode when virus definitions are updated
- About quarantining unrepairable infected files when operating in 7-Mode
- Specifying which embedded files to scan when operating in 7-Mode
- About configuring the client NetApp storage system operating in 7-Mode
- About verifying that the protection engine is registered with the storage system in 7-Mode
- About activating virus scanning in 7-Mode
- About specifying the file extensions to be scanned on the NetApp storage system in 7-Mode
- About NetApp operating in 7-Mode working with unresponsive protection engines
- How virus scanning affects backups on the NetApp storage system when operating in 7-Mode
Symantec™ Protection Engine for Network Attached Storage provides virus scanning and repair capabilities for the NetApp® Data ONTAP® storage system operating in 7-Mode.

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

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

- Symantec Protection Engine version 7.8 provides the virus scanning and repair services. For more information, see Symantec™ Protection Engine for Network Attached Storage Implementation Guide included in the product zip file.
- NetApp® Data ONTAP™ version 7.3.7 and version 8.2.1 operating in 7-Mode. Some options are configured directly on the NetApp storage system. No additional code is necessary to connect Symantec Protection Engine to the NetApp storage system. See "About configuring the client NetApp storage system operating in 7-Mode".

**How Symantec Protection Engine works with the NetApp storage system operating in 7-Mode**

Symantec Protection Engine provides virus scanning and repair capabilities for NetApp® Data ONTAP™ version 7.3.7 and version 8.2.1 operating in 7-Mode.

Symantec Protection Engine must be installed on a computer that is running Windows 2008 or Windows 2012. Symantec Protection Engine 7.8 has been certified with Data ONTAP version 7.3.7 and version 8.2.1 operating in 7-Mode for the following Windows server platforms:

- Windows Server 2008 SP2 64-bit
- Windows Server 2008 R2 SP1 64-bit
- Windows Server 2012 (64 bit)

Symantec Protection Engine must be located in the same domain as the NetApp storage system for which it provides scanning and repair services. Symantec Protection Engine uses the proprietary Network Appliance adaptation of the RPC protocol to interface with the NetApp storage system.

A single Symantec Protection Engine can support multiple NetApp storage systems. You can use multiple protection 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 when operating in 7-Mode

The NetApp storage system can submit files to Symantec Protection Engine for scanning on open, read, rename and close. This can be also configured for the CIFS share.

When a user tries to access a file, the storage system passes the file to Symantec Protection Engine for scanning. After a file is scanned, Symantec Protection Engine indicates the scanning results to the storage system. If a file is infected and can be repaired, the protection 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 Protection Engine can be configured to quarantine these unrepairable files.

See "About quarantining unrepairable infected files when operating in 7-Mode"

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 Protection Engine are updated, the `vscan reset` command is run on the storage system, or when the NetApp storage system 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 limiting scanning by file type when operating in 7-Mode

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 protection engine by the NetApp storage system for scanning

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 Protection Engine

The NetApp storage system lets you specify by file extension the files that are to be passed to Symantec Protection 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 in 7-Mode"

Symantec Protection 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 can configure which embedded files are scanned through the Symantec Protection Engine administrative interface.

See "Specifying which embedded files to scan when operating in 7-Mode"
About handling infected files when operating in 7-Mode

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

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

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

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

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

See "About quarantining unrepairable infected files when operating in 7-Mode”

About user identification and notification when a virus is found when operating in 7-Mode

When a virus is found in a file that is requested from the NetApp storage system, Symantec Protection 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 the Infection Found log messages that is logged to the local logs, Windows Event Log, SMTP, and SNMP.

**Note:** Symantec Protection 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 storage system is omitted from the log messages and from the user notification window.

You also can configure Symantec Protection 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 Protection Engine, and on the computer of the user.

See "Notifying a requesting user that a virus is found when operating in 7-Mode”
About preparing for installation when operating in 7-Mode

If you plan to use a single Symantec Protection Engine to support multiple storage systems, each storage system must support Data ONTAP version 7.3.7 and version 8.2.1 operating in 7-Mode. As a prerequisite, ensure that each NetApp storage system for which the protection engine is to provide scanning and repair services meets this requirement.

See "Before you install Symantec Protection Engine"

See "System requirements to install Symantec Protection Engine on Windows"

See "About installing Symantec Protection Engine"

See "Installing Symantec Protection Engine on Windows"

After you install Symantec Protection Engine, configure the NetApp storage system to work with the protection engine.

See "About configuring the client NetApp storage system operating in 7-Mode"

For the upgrade process and post installation steps, please refer to the Symantec™ Protection Engine for Network Attached Storage Implementation Guide included in product zip file.

About configuring Symantec Protection Engine to work with NetApp operating in 7-Mode

Configure Symantec Protection 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 XML modifier commands. Then you can configure the RPC-specific options.

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

See "Editing the service start-up properties"

Notifying the NetApp storage system operating in 7-Mode when virus definitions are updated

When Symantec Protection Engine scans a file, the scan status is stored in the cache of the NetApp storage system.

You can configure the protection engine to automatically notify the NetApp storage system when the protection 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 protection engine again for scanning.

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 of the NetApp storage system operating in 7-Mode"

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 operating in 7-Mode when virus definitions are updated

1. Go to Symantec Protection Engine installation directory.
2. Use the following xmlmodifier command

```
XMLModifier.exe -s
/configuration/ProtocolSettings/RPC/AutomaticSendVirusUpdatesEnabled/@value true
configuration.xml
```

3. Restart Symantec Protection Engine service.

# About quarantining unrepairable infected files when operating in 7-Mode

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 or Windows 2003. Symantec Central Quarantine is included on the Symantec Protection Engine distribution zip file along with supporting documentation.

Symantec Protection 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* included in the product zip file.

## To configure the quarantine server in Symantec Protection Engine

1. Go to Symantec Protection Engine installation directory.
2. Enable the quarantine settings.

**Command:**

```
xmlmodifier -s //configuration/QuarantineServerSettings/@enabled true configuration.xml
```

**Allowed values:**
- False: Disables quarantine.
- True: Enables quarantine.

**Default value:** false

3. Specify the quarantine server name.

**Command:**

```
xmlmodifier -s //configuration/QuarantineServerSettings/ServerName/@value <server name> configuration.xml
```

**Allowed values:**
Hostname or IP address for the computer on which Symantec Central Quarantine Server is installed.

4. Specify the quarantine server port.

```
xmlmodifier -s //configuration/QuarantineServerSettings/ServerPort/@value <value> configuration.xml
```
For example, xmlmodifier -s //configuration/QuarantineServerSettings/ServerPort/@value 4200 configuration.xml

**Allowed values:**
TCP/IP port number that Symantec Protection Engine uses to pass files to Symantec Central Quarantine.

5. Restart Symantec Protection Engine service.

### To quarantine unrepairable infected files

1. Go to Symantec Protection Engine installation directory.
2. Execute the following command:
   XMLModifier.exe -s /policies/ThreatPolicies/Actions/Quarantine/@value true policy.xml
3. Restart Symantec Protection Engine service.

### Specifying which embedded files to scan when operating in 7-Mode

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 Protection Engine is configured by default to scan all files.

#### To specify which files to scan

1. Go to Symantec Protection Engine installation directory.
2. Enable extension policy to scan all files except those in the extension or type exclude lists.
   
   **Command:**
   xmlmodifier -s //policies/ThreatPolicies/ExtensionPolicy/@value 2 policy.xml
   
   **Allowed values:**
   - 0 – Disable
   - 2 – Enable
   
   **Default value:** 0
3. You can add or remove any file extension that you want to exclude form AV scanning at the below XPath in the policy.xml file.
   
   **XPath:**
   //policies/ThreatPolicies/ExcludeList
   
   **Allowed values:** For allowed values, refer Implementation Guide.
4. You can add or remove entries in the file type exclude list in the policy.xml at the below XPath:
   
   **XPath:**
   //policies/ThreatPolicies/MIMEExcludeList
   
   **Allowed values:** Valid MIME file type
5. After running all the required commands, restart Symantec Protection Engine service.
For more information please refer “Specify which files to scan” in Symantec Protection Engine 7.8.0 Implementation Guide.

### About configuring the client NetApp storage system operating in 7-Mode

After you configure Symantec Protection Engine to use RPC as the communication protocol, you must configure the NetApp storage systems operating in 7-Mode to work with Symantec Protection Engine.

The NetApp storage systems must be running Data ONTAP version 7.3.7 or version 8.2.1 operating in 7-Mode to interface with Symantec Protection Engine. If you plan to support more than one storage system with a single protection engine, each storage system must be running Data ONTAP version 7.3.7 or version 8.2.1 operating in 7-Mode.

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 Protection Engine.

### About verifying that the protection engine is registered with the storage system in 7-Mode

You can verify that the protection engine is registered with the storage system operating in 7-Mode after you install Symantec Protection Engine. Registration is automatic if you have provided the correct information to Symantec Protection Engine for contacting the storage system. Registration occurs when the protection engine connects to the storage system. Use the `vscan` command at the command line interface to check the list of registered protection engines.

Note: The service startup properties for Symantec Protection 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 protection engine cannot register with the storage system because it does not have sufficient permission.

See "Editing the service start-up properties"

### About activating virus scanning in 7-Mode

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 in 7-Mode

Configure the list of extensions on the NetApp storage system in 7-Mode to contain only the file extensions that you want to scan. This lets you control the file types that are passed to Symantec Protection Engine for scanning. You can configure file extensions using the extensions include and exclude list. The extensions that are configured on
Symantec Protection Engine have preference over the file types and the extensions configured on the NetApp storage system. For example, if .doc is included in the extensions exclude list for Symantec Protection Engine but is included on the NetApp storage system, the .doc file is not 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.

---

**Note:** If a container file (for example, a .zip or .lzh file) is included in the extensions exclude list for Symantec Protection Engine, the child files contained within the container file will get scanned unless the extensions of the child files are included in the extensions exclude 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 roll back 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 appropriate NetApp storage system documentation.

### About NetApp operating in 7-Mode working with unresponsive protection engines

The NetApp storage system operating in 7-Mode can be configured to let the connection time out while waiting for a reply from Symantec Protection 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 enables Windows Messenger Loggings to see if the protection engine is currently at work on its request. If there is still no response, the storage system sends the scan request to another protection engine.

If none of the protection engines respond, 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 appropriate NetApp storage system documentation.

### How virus scanning affects backups on the NetApp storage system when operating in 7-Mode

The service startup properties for Symantec Protection Engine must be edited to identify an account with Backup Operator privileges on the NetApp storage system when operating in 7-Mode. Otherwise, backups on the storage system might not finish successfully when virus scanning is active.
The NetApp storage system when operating in 7-Mode can time out while waiting for a reply from the Symantec Protection 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 when operating in 7-Mode.

See "Editing the service start-up properties"

---

**About clearing the scanned files cache of the NetApp storage system operating in 7-Mode**

When Symantec Protection Engine scans a file, the scan status is stored in the cache of the NetApp storage system operating in 7-Mode. Symantec Protection Engine automatically notifies the NetApp storage system when the protection 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 protection engine again for scanning.

See "Notifying the NetApp storage system operating in 7-Mode when virus definitions are updated"

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 when operating in 7-Mode**

You can configure Symantec Protection 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 is found when operating in 7-Mode"

You can also enable the NetApp storage system to display warning messages by the `vscan options client_msgbox {on|off}` command.

---

**About specifying which embedded files to scan**

The NetApp storage system submits files to Symantec Protection 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's administrative interface. The top-level files that are sent to Symantec Protection Engine are scanned regardless of file extension.

When the protection 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 protection engine's 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 Protection 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 must scan all files even if you normally control the file types that are scanned with the file type or file extension exclusion list.
Configuring Symantec™ Protection Engine for Network Attached Storage 7.8 for NetApp® clustered Data ONTAP®

This chapter includes the following topics:

- About software components for NetApp® clustered Data ONTAP®
- How Symantec Protection Engine works with the NetApp system running clustered Data ONTAP
- About NetApp® clustered Data ONTAP®
- What happens when a file is scanned when operating with clustered Data ONTAP
- About limiting scanning by file type for clustered Data ONTAP
- About handling infected files for clustered Data ONTAP
- About user identification and notification when a virus is found for clustered Data ONTAP
- About preparing for installation for clustered Data ONTAP
- About configuring Symantec Protection Engine to work with NetApp clustered Data ONTAP
- Notifying the NetApp system running clustered Data ONTAP when virus definitions are updated
- About quarantining unrepairable infected files for system running clustered Data ONTAP
- Specifying which embedded files to scan for clustered Data ONTAP
- About configuring the client NetApp system running clustered Data ONTAP
- About verifying that the protection engine is registered with the NetApp system running clustered Data ONTAP
- About activating virus scanning on the system running clustered Data ONTAP
- About specifying the file extensions to be scanned on the NetApp system running clustered Data ONTAP
About software components for NetApp® clustered Data ONTAP®

Configure the following components to add antivirus scanning to the NetApp system running clustered Data ONTAP:

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

- Symantec Protection Engine version 7.8 provides the virus scanning and repair services. For more information, see Symantec™ Protection Engine for Network Attached Storage Implementation Guide included in the product zip file.
- NetApp® clustered Data ONTAP™ version 8.2.1. Some options are configured directly on the NetApp storage system. No additional code is necessary to connect Symantec Protection Engine to the NetApp storage system. See

How Symantec Protection Engine works with the NetApp system running clustered Data ONTAP

Symantec Protection Engine provides virus scanning and repair capabilities for NetApp® clustered Data ONTAP™ version 8.2.1.

Symantec Protection Engine must be installed on a computer that is running Windows 2008 or Windows 2012. Symantec Protection Engine 7.8 has been certified with clustered Data ONTAP version 8.2.1 for the following Windows server platforms:

- Windows 2008 SP2 64-bit
- Windows 2008 R2 SP1 64-bit
- Windows Server 2012 (64 bit)

Symantec Protection Engine must be located in the same domain as the NetApp storage system for which it provides scanning and repair services. Symantec Protection Engine uses the proprietary Network Appliance adaptation of the RPC protocol to interface with the NetApp storage system.
A single Symantec Protection Engine can support multiple NetApp storage systems. You can use multiple protection 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.

### About NetApp® clustered Data ONTAP®

Symantec Protection Engine can scan files from NetApp storage devices configured to work in a cluster.

**Components**

- **Storage Virtual Machine:** Storage Virtual Machine (SVM), formerly known as Vserver, is a virtual machine that provides network access through unique network addresses that might serve data out of a distinct namespace, and that can be separately administered from the rest of the cluster. There are three types of SVMs: admin, node, and data. Unless there is a specific need to identify the type of SVM, SVM usually refers to the data SVM.
- **Vscanner:** Windows server which is used for Antivirus scanning
- **Vscan engine:** Symantec Protection Engine, running on the vscanner
- **clustered Data ONTAP Antivirus Connector:** Antivirus connector running on the same vscanner
- **Logical interface (LIF):** IP address used to access the cluster/Cluster management Host

The antivirus connector needs to be provided with the IP address of one or more cluster management hosts, each of which can be for a single SVM, or an entire cluster. The antivirus connector queries each management host for a list of SVM data LIFs, which the connector will attempt to register with, at most one connection per SVM per node. Each SVM must be provided with the IP address of one or more Vscanners. ONTAP will reject any attempt to register as a Vscanner if the server is not in the list of allowed Vscanners. Additionally, the account used by the Vscanner for privileged access (ontap_admin$) must be a configured account. The Vscanner can handle requests from more than one SVM. A single antivirus connector can be configured to handle an arbitrary number of SVMs, and that is transparent to the Vscan engine. The antivirus connector deals with all notification traffic between the cluster and the Vscanner. The antivirus connector handles the reconnection to the Vscan engine after a failover. If any I/O from the Vscan engine is disrupted by the failover, the Vscan engine should report the error response to the antivirus connector. The antivirus connector will deal with retries in this situation.

Symantec Protection Engine should be able to handle clustered Data ONTAP and 7-Mode scanning simultaneously. The loopback connection would be used for all clustered Data ONTAP requests, and the 7-Mode connections would be handled as mentioned in the previous sections.

See "How Symantec Protection Engine works with the NetApp storage system operating in 7-Mode"

### What happens when a file is scanned when operating with clustered Data ONTAP

The NetApp storage system can submit files to Symantec Protection Engine for scanning on open, read, rename and close. This can be also configured for the CIFS share.

When a user tries to access a file, the storage system passes the file to Symantec Protection Engine for scanning. After a file is scanned, Symantec Protection Engine indicates the scanning results to the storage system. If a file is infected and can be repaired, the protection 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 Protection Engine can be configured to quarantine these unrepairable files.

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 Protection Engine are updated, the *vserver vscan reset* command is run on the storage system, or when the NetApp storage system 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 limiting scanning by file type for clustered Data ONTAP

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 protection 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 Protection 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 system running clustered Data ONTAP"

- **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 Protection Engine**
  - Symantec Protection 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 can configure which embedded files are scanned through the Symantec Protection Engine administrative interface.
  - See "Specifying which embedded files to scan for clustered Data ONTAP"

### About handling infected files for clustered Data ONTAP

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

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

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

- **Scan and repair or delete**
  - Scan for viruses. Try to repair the infected file, and delete any unrepairable file.
You can also configure the protection engine to quarantine unrepairable files.
See "About quarantining unrepairable infected files for system running clustered Data ONTAP"

**About user identification and notification when a virus is found for clustered Data ONTAP**

When a virus is found in a file that is requested from the NetApp storage system, Symantec Protection 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 the Infection Found log messages that is logged to the local logs, Windows Event Log, SMTP, and SMNP.

---

**Note:** Symantec Protection 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 storage system is omitted from the log messages and from the user notification window.

You also can configure Symantec Protection 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 Protection Engine, and on the computer of the user.

See "Notifying a requesting user that a virus is found for clustered Data ONTAP"

**About preparing for installation for clustered Data ONTAP**

If you plan to use a single Symantec Protection Engine to support multiple storage systems, each storage system must support clustered Data ONTAP version 8.2.1. As a prerequisite, ensure that each NetApp storage system for which the protection engine is to provide scanning and repair services meets this requirement.

See "Before you install Symantec Protection Engine"
See "System requirements to install Symantec Protection Engine on Windows"
See "About installing Symantec Protection Engine"
See "Installing Symantec Protection Engine on Windows"

After you install Symantec Protection Engine, configure the NetApp storage system to work with the protection engine.

See "About configuring the client NetApp system running clustered Data ONTAP"

For the upgrade process and post installation steps, please refer to the Symantec™ Protection Engine for Network Attached Storage Implementation Guide included in product zip.

About configuring Symantec Protection Engine to work with NetApp clustered Data ONTAP

Configure Symantec Protection 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.

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

See "Editing the service start-up properties"

Notifying the NetApp system running clustered Data ONTAP when virus definitions are updated

When Symantec Protection Engine scans a file, the scan status is stored in the cache of the NetApp system running clustered Data ONTAP.

You can configure the protection engine to automatically notify the NetApp storage system when the protection 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 protection engine again for scanning.

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 of the NetApp system running clustered Data ONTAP"

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 system running clustered Data ONTAP when virus definitions are updated

1. Go to Symantec Protection Engine installation directory.
2. Use the following xml modifier command
   XMLModifier.exe -s /configuration/ProtocolSettings/RPC/AutomaticSendVirusUpdatesEnabled/@value true configuration.xml
3. Restart Symantec Protection Engine service.

To manually notify the NetApp system running clustered Data ONTAP when virus definitions are updated
1. Go to Symantec Protection Engine installation directory.

2. Use the following xml modifier command:

```
XMLModifier.exe -s
/configuration/ProtocolSettings/RPC/AutomaticSendVirusUpdatesEnabled/@value true
configuration.xml
```

3. Restart Symantec Protection Engine service.

### About quarantining unrepairable infected files for system running clustered Data ONTAP

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 or Windows 2003. Symantec Central Quarantine is included on the Symantec Protection Engine distribution zip file along with supporting documentation.

Symantec Protection 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* included in the product zip file.

### To configure the quarantine server in Symantec Protection Engine

1. Go to Symantec Protection Engine installation directory.
2. Enable the quarantine settings.

**Command:**
```
xmllmodifer -s //configuration/QuarantineServerSettings/@enabled true configuration.xml
```

**Allowed values:**
- False: Disables quarantine.
- True: Enables quarantine.

**Default value:** false

3. Specify the quarantine server name.

**Command:**
```
xmllmodifer -s //configuration/QuarantineServerSettings/ServerName/@value <server name>
configuration.xml
```

**Allowed values:**
Hostname or IP address for the computer on which Symantec Central Quarantine Server is installed.

4. Specify the quarantine server port.
xmlmodifier -s //configuration/QuarantineServerSettings/ServerPort/@value <value> onfigurati
configuration.xml

For example,
xmlmodifier -s //configuration/QuarantineServerSettings/ServerPort/@value 4200 configuration.xml

**Allowed values:**
TCP/IP port number that Symantec Protection Engine uses to pass files to Symantec Central Quarantine.

5. Restart Symantec Protection Engine service.

**To quarantine unrepairable infected files**

1. Go to Symantec Protection Engine installation directory.
2. Execute the following command:
   XMLModifier.exe -s /policies/ThreatPolicies/Actions/Quarantine/@value true policy.xml
3. Restart Symantec Protection Engine service.

**Specifying which embedded files to scan for clustered Data ONTAP**

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 Protection Engine is configured by default to scan all files.

**To specify which files to scan**

1. Go to Symantec Protection Engine installation directory.
2. Enable extension policy to scan all files except those in the extension or type exclude lists.
   Command:
   xmlmodifier -s //policies/ThreatPolicies/ExtensionPolicy/@value 2 policy.xml
   **Allowed values:**
   - 0 – Disable
   - 2 – Enable
   Default value: 0
3. You can add or remove any file extension that you want to exclude form AV scanning at the below XPath in the policy.xml file.
   XPath:
   //policies/ThreatPolicies/ExcludeList
   **Allowed values:** For allowed values, refer Implementation Guide.
4. You can add or remove entries in the file type exclude list in the policy.xml at the below XPath:
   XPath:
   //policies/ThreatPolicies/MIMEExcludeList
   **Allowed values:** Valid MIME file type
5. Restart Symantec Protection Engine service.
   For more information, refer “Specify which files to scan” in Symantec Protection Engine 7.8.0 Implementation Guide.

About configuring the client NetApp system running clustered Data ONTAP

After you configure Symantec Protection Engine to use RPC as the communication protocol, you must configure the NetApp system running clustered Data ONTAPs to work with Symantec Protection Engine.

The NetApp storage systems must be running clustered Data ONTAP version 8.2.1 to interface with Symantec Protection Engine version 7.8. If you plan to support more than one storage system with a single protection engine, each storage system must be running clustered Data ONTAP version 8.2.1.

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 Protection Engine.

About verifying that the protection engine is registered with the NetApp system running clustered Data ONTAP

You can verify that the protection engine is registered with the system running clustered Data ONTAP after you install Symantec Protection Engine. Registration is automatic if you have provided the correct information to Symantec Protection Engine for contacting the storage system. Registration occurs when the protection engine connects to the storage system.

Note: The service startup properties for Symantec Protection 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 protection engine cannot register with the storage system because it does not have sufficient permission.

About activating virus scanning on the system running clustered Data ONTAP

You can activate and deactivate virus scanning. Use the `vserver vscan enable` command at the command line to activate virus scanning. Use the `vserver vscan disable` command to deactivate virus scanning.

About specifying the file extensions to be scanned on the NetApp system running clustered Data ONTAP

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 Protection Engine for scanning. By default, all files extensions are included for scanning. The extensions that are configured on Symantec Protection Engine have preference over the file types and the extensions configured on the NetApp storage system. For example, if `.doc` is
included in the extensions exclude list for Symantec Protection Engine but is included on the NetApp storage system, the .doc file is not scanned.

For the extensions exclude list, the `vserver vscan on-access-policy create` or the `vserver vscan on-access-policy modify` command would add extensions to the exclude list or remove extensions from the exclude list on the NetApp storage system.

The wildcard extension * and ? are supported for extensions-to-exclude parameter of `on-access policy create` and `on-access policy modify` commands. The wildcard extensions scan all files regardless of file extension, which 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 appropriate NetApp storage system documentation.

### About NetApp clustered Data ONTAP working with unresponsive protection engines

The NetApp system running clustered Data ONTAP can be configured to let the connection time out while waiting for a reply from Symantec Protection 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 `vserver vscan scanner-pool create` or the `vserver vscan scanner-pool modify` command. The default value is 10 seconds. When the scan request times out, the NetApp storage system enables Windows Messenger Loggings to see if the protection engine is currently at work on its request. If there is still no response, the storage system sends the scan request to another protection engine.

If none of the protection engines respond, the NetApp storage system can either allow file access without virus scanning or deny file access altogether. Configure this option by using the `vserver vscan on-access-policy create` or the `vserver vscan on-access-policy modify` command.

You can end a virus scanning session by using the `vserver vscan scanner-pool modify` or the `vserver vscan scanner-pool servers remove` command.

You can also allow the scan pool to be idle by using the `vserver vscan scanner-pool apply-policy` command.

For more information, see the appropriate NetApp storage system documentation.

### How virus scanning affects backups on the NetApp system running clustered Data ONTAP

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

The NetApp system running clustered Data ONTAP can time out while waiting for a reply from the Symantec Protection 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 system running clustered Data ONTAP.
About clearing the scanned files cache of the NetApp system running clustered Data ONTAP

When Symantec Protection Engine scans a file, the scan status is stored in the cache of the system running clustered Data ONTAP. Symantec Protection Engine automatically notifies the NetApp storage system when the protection 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 protection engine again for scanning.

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

About notifying a requesting user that a virus was found for clustered Data ONTAP

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

You can also enable the system running clustered Data ONTAP to display warning messages by the `vscan options client_msgbox {on|off}` command.

About specifying which embedded files to scan

The NetApp storage system submits files to Symantec Protection 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's administrative interface. The top-level files that are sent to Symantec Protection Engine are scanned regardless of file extension.

When the protection 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 protection engine's 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 Protection 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 must scan all files even if you normally control the file types that are scanned with the file type or file extension exclusion list.

About configuration options

To modify an XML file, you must know the XPath and the field values.
You can use the XML modifier command-line tool of Symantec Protection Engine to configure the following options:

- To enable the granular scan status is Cluster mode See "Enable granular scan status for clustered Data ONTAP"
- To specify the client logging information in log files See "Specify client information logging in log files"
- To specify the notification threshold in case of overload See "Specify notification threshold is case of overload"

## Enable granular scan status for clustered Data ONTAP

Use this option to enable granular scan status for clustered Data ONTAP. Symantec Protection Engine registers with scanning functionality and reports the granular status.

**Granular scan status setting** lists the granular scan status setting for clustered Data ONTAP

### Table 4-1  Granular scan status setting

<table>
<thead>
<tr>
<th>XPath</th>
<th>Field values</th>
<th>Default values</th>
</tr>
</thead>
<tbody>
<tr>
<td>/configuration/ProtocolSettings/RPC/</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EnableGranularScanStatus</td>
<td>• True - Enables Symantec Protection Engine to send the granular scan status for clustered Data ONTAP&lt;br&gt;• False - Disables Symantec Protection Engine from sending the granular scan status for clustered Data ONTAP</td>
<td>true</td>
</tr>
</tbody>
</table>

## Specify client information logging in log files

Symantec Protection Engine, by default, logs client information when a policy violation is detected.

**Logging client information setting** lists the setting to log client information when a policy violation is detected.

### Table 4-2  Logging client information setting

<table>
<thead>
<tr>
<th>XPath</th>
<th>Field values</th>
<th>Default values</th>
</tr>
</thead>
<tbody>
<tr>
<td>/configuration/ProtocolSettings/RPC/</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LogClientInformationForCleanFiles</td>
<td>• True - Logs client information for all files&lt;br&gt;• False - Logs client information only when a policy violation is detected</td>
<td>false</td>
</tr>
</tbody>
</table>
Specify notification threshold in case of overload

Note: This option is only applicable for the RPC protocol.

Use this option to send a notification to the specified logging destinations when it reaches its scan queued requests threshold. Symantec Protection Engine then rejects requests and sends notification that the threshold is reached. This feature lets the client determine load balancing and prevents the server from being overloaded with scan requests.

Note: You must first enable the Enable Granular Scan Status parameter by setting it to true. For example, EnableGranularScanStatus = true.

Notification threshold setting lists the notification threshold setting

<table>
<thead>
<tr>
<th>XPath</th>
<th>Field values</th>
<th>Default values</th>
</tr>
</thead>
<tbody>
<tr>
<td>/configuration/ ProtocolSettings/</td>
<td></td>
<td>true</td>
</tr>
<tr>
<td>EnableServerTooBusyResponse</td>
<td>• True - Enables Symantec Protection Engine to send a notification when the</td>
<td></td>
</tr>
<tr>
<td></td>
<td>queued requests reach threshold</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• False - Disables Symantec Protection Engine from sending a notification when</td>
<td></td>
</tr>
<tr>
<td></td>
<td>the queued requests reach threshold</td>
<td></td>
</tr>
</tbody>
</table>

Specify scanning via encoded path

Symantec Protection Engine, by default, enables scanning of files via their encoded paths. Scanning via the encoded path setting lists the setting to scan files via the encoded path.

<table>
<thead>
<tr>
<th>XPath</th>
<th>Field values</th>
<th>Default values</th>
</tr>
</thead>
<tbody>
<tr>
<td>/configuration/ ProtocolSettings/RPC/</td>
<td></td>
<td>true</td>
</tr>
<tr>
<td>EncodedPaths</td>
<td>• True - Enables the scanning of files via the encoded</td>
<td></td>
</tr>
<tr>
<td></td>
<td>path</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• False - Disables the scanning of files via the encoded</td>
<td></td>
</tr>
<tr>
<td></td>
<td>path</td>
<td></td>
</tr>
</tbody>
</table>