Configuring Symantec™ Protection Engine for Network Attached Storage 7.5 for NetApp® Data ONTAP®
Configuring Symantec™ Protection Engine for Network Attached Storage 7.5 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.

Documentation version: 7.5

Legal Notice

Copyright © 2014 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.
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:

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, 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
Europe, Middle-East, and Africa  seMEA@symantec.com
North America and Latin America  supportSolutions@symantec.com
### Technical Support

#### Chapter 1 Installing and configuring Symantec™ Protection Engine for Network Attached Storage 7.5

- Before you install Symantec Protection Engine .................................................. 10
- System requirements to install Symantec Protection Engine on Windows ................ 12
- About installing Symantec Protection Engine ..................................................... 13
  - Installing Symantec Protection Engine on Windows ........................................ 15
- Editing the service start-up properties ............................................................... 20
- Accessing the console ....................................................................................... 21
- About configuring the RPC protocol options .................................................... 22
  - Configuring the RPC protocol options ............................................................. 23
- Scheduling LiveUpdate to update virus definitions automatically ...................... 27
- Configuring Rapid Release updates to occur automatically ............................. 29
- About connecting to Symantec Protection Engine ............................................. 30

#### Chapter 2 Configuring Symantec™ Protection Engine for Network Attached Storage 7.5 for NetApp® Data ONTAP® operating in 7-Mode

- About software components for NetApp® Data ONTAP® when operating in 7-Mode ........................................................................................................ 32
- How Symantec Protection Engine works with the NetApp storage system operating in 7-Mode ......................................................................................... 32
- What happens when a file is scanned when operating in 7-Mode ......................... 33
- About limiting scanning by file type when operating in 7-Mode ......................... 33
- About handling infected files when operating in 7-Mode .................................... 34
- About user identification and notification when a virus is found when operating in 7-Mode .............................................................................................. 35
- About preparing for installation when operating in 7-Mode ............................... 36
- About configuring Symantec Protection Engine to work with NetApp operating in 7-Mode .............................................................................................. 36
Notifying the NetApp storage system operating in 7-Mode when virus definitions are updated ................................................................. 37
About quarantining unrepairable infected files when operating in 7-Mode ......................................................................................... 38
Specifying which embedded files to scan when operating in 7-Mode ................................................................................................. 46
About configuring the client NetApp storage system operating in 7-Mode ......................................................................................... 42
About verifying that the protection engine is registered with the storage system in 7-Mode ................................................................. 42
About activating virus scanning in 7-Mode ........................................................................................................................................ 43
About specifying the file extensions to be scanned on the NetApp storage system in 7-Mode ............................................................. 43
About NetApp operating in 7-Mode working with unresponsive protection engines ........................................................................ 44
How virus scanning affects backups on the NetApp storage system when operating in 7-Mode .......................................................... 44
About clearing the scanned files cache of the NetApp storage system operating in 7-Mode ................................................................. 45
About notifying a requesting user that a virus was found when operating in 7-Mode ........................................................................ 45
About specifying which embedded files to scan .................................................................................................................................. 64
Specifying which embedded files to scan when operating in 7-Mode ................................................................................................. 46

Chapter 3 Configuring Symantec™ Protection Engine for Network Attached Storage 7.5 for NetApp® clustered Data ONTAP® ................................................ 49
About software components for NetApp® clustered Data ONTAP® ........................................................................................................ 50
How Symantec Protection Engine works with the NetApp system running clustered Data ONTAP .......................................................... 50
About NetApp® clustered Data ONTAP® ........................................................................................................................................ 51
What happens when a file is scanned when operating with clustered Data ONTAP .................................................................................. 52
About limiting scanning by file type for clustered Data ONTAP ........................................................................................................ 52
About handling infected files for clustered Data ONTAP ..................................................................................................................... 53
About user identification and notification when a virus is found for clustered Data ONTAP ........................................................................ 54
About preparing for installation for clustered Data ONTAP ................................................................................................................ 55
Installing and configuring Symantec™ Protection Engine for Network Attached Storage 7.5

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
- Editing the service start-up properties
- Accessing the console
- About configuring the RPC protocol options
- Scheduling LiveUpdate to update virus definitions 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” on page 12.

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

- On Windows operating system, if you want to use Windows Active Directory-based authentication method to access the Symantec Protection Engine console, you must ensure the following:
  - Create or identify an existing security group in the Active Directory that would be authorized to access the Symantec Protection Engine console.
  - The server (on which you plan to install Symantec Protection Engine) belongs to the same domain or has trust relationship with the Active Directory, that contains the security group authorized to access the Symantec Protection Engine console.

- Install Java 2SE Runtime Environment (JRE) 7.0 (update 45 or later).

  **Note:** Symantec Protection Engine supports only 32-bit versions of Java Runtime Environment. Symantec Protection Engine cannot be installed with 64-bit JRE versions.

- 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

The minimum system requirements to install Symantec Protection Engine on Windows are as follows:

**Operating system**
- Windows Server 2008 SP2 (32-bit and 64-bit)
- Windows Server 2008 R2 (64-bit)
- Windows Server 2008 Japanese (32-bit and 64-bit)
- Windows Server 2008 R2 Japanese (64-bit)
- Windows Server 2012 (64-bit)
- Windows Server 2012 R2 (64-bit)
- Windows Server 2012 Japanese (32-bit and 64-bit)

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**
- 4 GB RAM or higher

**Disk space**
- 5 GB of hard disk space
- 10 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)
Software

- JRE 7.0 (update 45 or later)
  Note: You must install JRE only if you plan to operate Symantec Protection Engine in the Core server with user interface mode.
  
  Note: Symantec Protection Engine supports only 32-bit versions of Java Runtime Environment. Symantec Protection Engine cannot be installed with 64-bit JRE versions.

- Microsoft Visual C++ 2010 (SP1 or later) redistributable package (x86)

- One of the following Web browsers to access the Symantec Protection Engine console:
  - Microsoft Internet Explorer 10 or later
    Use Microsoft Internet Explorer to access the Symantec Protection Engine console from a Windows client computer.
  - Mozilla Firefox 10 or later
    Use Mozilla Firefox to access the Symantec Protection Engine console from a Solaris or Linux client computer.

The Web browser is required only for Web-based administration. You must install the Web browser on a computer from which you want to access the Symantec Protection Engine console. The computer must have access to the server on which Symantec Protection Engine runs.

Hypervisor support

- VMWare® vSphere Hypervisor™ version 5.1 or later
- Windows 2008 R2 Hyper-V
- Windows 2012 Hyper-V
- Xen 3.4.3 (installed on RHEL 5.4, 64-bit)

The following Windows guest operating systems have been certified on Hyper-V:

- Windows Server 2008 SP2 (32-bit and 64-bit)
- Windows Server 2008 R2 (64-bit)
- Windows Server 2008 Japanese (32-bit and 64 bit)
- Windows Server 2008 R2 Japanese (64-bit)
- Windows Server 2012 (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.
Table 1-1 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>Version</th>
<th>Action taken by installer</th>
</tr>
</thead>
<tbody>
<tr>
<td>No previous version is detected</td>
<td>A full installation is performed</td>
</tr>
<tr>
<td>Version 7.0 is detected</td>
<td>Symantec Protection Engine supports an upgrade from version 7.0. You can select whether to upgrade the product and preserve your existing settings or to perform a clean upgrade. If you choose to do a clean upgrade, the installer removes the previous version, and then installs the newer version as a full installation, without preserving any previous settings.</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 or 5.2. You must first upgrade to version 7.0 and then further upgrade to version 7.5.</td>
</tr>
<tr>
<td>Version 5.0 is detected</td>
<td>Symantec Protection Engine does not support direct upgrades from version 5.0. To install version 7.5, you must first either uninstall version 5.0 or upgrade to version 7.0 and then further upgrade to version 7.5.</td>
</tr>
<tr>
<td>Version 4.3.x is detected</td>
<td>Symantec Protection Engine does not support direct upgrades from version 4.3.x. To install version 7.5, you must first either uninstall 4.3.x or upgrade to 5.2.x, then upgrade to 7.0, and then further upgrade to version 7.5.</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.

See “Installing Symantec Protection Engine on Windows” on page 15.

Installing Symantec Protection Engine on Windows

During installation, you can choose the authentication mode for accessing the Symantec Protection Engine console. If you choose Symantec Protection Engine-based authentication then Symantec Protection Engine installs an administrator account. Symantec recommends that you remember the password for this account as it is the only account used to manage Symantec Protection Engine. If you want to change the password in the console, you must have the old password.

If you choose Windows Active Directory-based authentication, Symantec Protection Engine allows users from the authorized Windows Active Directory security group to access the console.

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” on page 12.

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 with Symantec Protection Engine-based authentication

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

6 In the **Initialization Methods** panel, select one of the following options, and click **Next**:

- **Core server with user interface (requires JRE)**
  
  Select this option if you want to use the user-interface console of Symantec Protection Engine.
  
  This method requires JRE to be installed.
  
  Proceed to step 7.

- **Core server only (does not require JRE)**
  
  Select this option if you do not want to use the user-interface console of Symantec Protection Engine.
  
  This method does not require JRE to be installed.
  
  Proceed to step 12.

7 In the **UI Authentication method** panel, select **Symantec Protection Engine-based authentication**, and then click **Next**.
8 In the **Administrative UI Setup** panel, configure the following options:

- **Administrator Password**
  Type a password for the administrator account that you intend to use to manage Symantec Protection Engine.

- **Confirm Administrator Password**
  Confirm the password by typing it again.

9 Click **Next**.

10 In the **Administrative UI Setup** panel, configure the following options:

- **Administrator Port**
  Type the port number on which the Web-based console listens.
  If you change the port number, use a number that is greater than 1024 that is not in use by any other program or service. The default port number is 8004. You can disable the console by typing 0. If you disable the console, you can configure Symantec Protection Engine by editing the configuration file.

- **SSL Port**
  Type the Secure Socket Layer (SSL) port number on which encrypted files are transmitted for increased security.
  The default SSL port number is 8005. If this port is already in use, select an SSL port that is not in use by any other program or service. Use a port number that is greater than 1024.

11 Click **Next**.

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

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

13 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.

14 Select the Insight aggression level.

  If you set the level higher, Insight detects more files as malicious. Higher settings, however, return more false positives.

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

16 Click **Finish**.
To install Symantec Protection Engine on Windows with Windows Active Directory-based authentication

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


3. In the Welcome panel, click Next.

4. In the License Agreement panel, after you read the agreement, indicate that you agree with the terms of the Symantec Software License Agreement, and then click Next.

   The default setting is that you do not agree with the terms of the Symantec Software License Agreement. If you do not indicate that you agree, the installation is canceled.

5. In the Destination Folder panel, select the location to install Symantec Protection Engine, and then click Next.

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

   **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.
6 In the **Initialization Methods** panel, select one of the following options, and click **Next**:

- **Core server with user interface (requires JRE)**
  
  Select this option if you want to use the user-interface console of Symantec Protection Engine.
  
  This method requires you to install JRE.
  
  Proceed to step 7.

- **Core server only (does not require JRE)**
  
  Select this option if you do not want to use the user-interface console of Symantec Protection Engine.
  
  This method does not require JRE to be installed.
  
  Proceed to step 12.

7 In the **UI Authentication method** panel, select **Windows Active Directory-based authentication**, and then click **Next**.

8 In the **Windows Active Directory-based Authentication Settings** panel, in the **Group Name** box, type a valid security group name in the **Domain\Groupname** format.

9 Click **Next**.

   If the group name is incorrect, a **Group Name Validation** screen appears.
   
   Click **Back** to try the security group name again.

   Alternatively, click **Next** to continue the installation without a valid group name.

   The Symantec Protection Engine service starts after installation but you cannot access the console. Once the installation is complete, you must go to configuration.xml and enter the user name to access the console.
10 In the **Administrative UI Setup** panel, configure the following options:

**Administrator Port** Type the port number on which the Web-based console listens.

If you change the port number, use a number that is greater than 1024 that is not in use by any other program or service. The default port number is 8004. You can disable the console by typing 0. If you disable the console, you can configure Symantec Protection Engine by editing the configuration file.

**SSL Port** Type the Secure Socket Layer (SSL) port number on which encrypted files are transmitted for increased security.

The default SSL port number is 8005. If this port is already in use, select an SSL port that is not in use by any other program or service. Use a port number that is greater than 1024.

11 Click **Next**.

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

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

13 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.

14 Select the Insight aggression level.

If you set the level higher, Insight detects more files as malicious. Higher settings, however, return more false detections.

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

16 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 (32-bit and 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*.

---

**Accessing the console**

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

---

**Note:** Symantec Protection Engine no longer supports accessing the console through an HTTP server.

The first time that you access the Symantec Protection 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 Protection Engine.

2. In the Web browser, type the following address:
   
   \[ \text{https://<servername>:<port>/} \]

   where `<servername>` is the host name or IP address of the server that is running Symantec Protection Engine and `<port>` is the port number that you selected during installation for the built-in Web server. The default port number is 8004.

3. If a **Security Alert** dialog box appears, click **Yes** to confirm that you trust the integrity of the applet, and then click **Yes** to display the Web page.

4. In the **Enter Password** box, type the password for the administrative account.

5. Press **Enter**.

**About configuring the RPC protocol options**

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

*Table 1-2* describes the protocol-specific options for RPC.
Table 1-2  Protocol-specific options for RPC

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RPC client list</td>
<td>A single Symantec Protection Engine can support one or more NetApp storage systems. The NetApp storage systems must be located in the same domain as the protection engine. You must provide the IP address of each NetApp storage system. Enter 127.0.0.1 in RPC client list to be able to operate with NetApp Clustered Data ONTAP. <strong>Note:</strong> Multiple protection engines can support a single NetApp storage system. Configure the scan engines through the NetApp storage system interface.</td>
</tr>
<tr>
<td>Check RPC connection every ___ seconds</td>
<td>Symantec Protection Engine maintains a connection with the NetApp storage system. Symantec Protection 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.</td>
</tr>
<tr>
<td>Maximum number of reconnect attempts</td>
<td>You can configure the protection engine to make a specified number of tries to re-establish a lost connection with the NetApp storage system. By default, Symantec Protection Engine is configured to try to reconnect with the NetApp storage system indefinitely. <strong>Note:</strong> Do not set a maximum number of reconnect attempts if the protection engine provides scanning for multiple NetApp storage systems. Use the default setting.</td>
</tr>
<tr>
<td>Automatically send antivirus update notifications</td>
<td>You can configure Symantec Protection 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.</td>
</tr>
</tbody>
</table>
| Antivirus scan policy                | You can configure Symantec Protection Engine to do one of the following when an infected file is found:  
  ■ Scan only  
  ■ Scan and repair files  
  ■ Scan and repair or delete |

Configuring the RPC protocol options

To configure RPC, do the following:
Provide an IP address for each NetApp storage system for which Symantec Protection Engine should provide scanning services. You can add or delete the storage systems from this list at any time.
Enter 127.0.0.1 in RPC client list to be able to operate with NetApp Clustered Data ONTAP.

- Configure the additional RPC-specific options.
- Configure the antivirus scan policies.

To edit the list of NetApp storage systems

1. On the Symantec Protection 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 Protection 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 Protection Engine should provide scanning services. Type one entry per line.

Enter 127.0.0.1 in RPC client list to be able to operate with NetApp Clustered Data ONTAP.
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 Protection 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 Protection Engine should check 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 Protection Engine should undertake to re-establish a lost connection with the NetApp storage system.

The default setting is 0. Symantec Protection Engine tries indefinitely to re-establish a connection. Use the default setting if the protection engine provides scanning for multiple NetApp storage systems.

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. You must perform a manual restart for the changes to take place and for a proper connection to the NetApp storage system.

To configure the antivirus scan policy

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

2 Under Views, click Scanning.
3 Select the **Antivirus scan policy** to configure Symantec Protection Engine to do one of the following when an infected file is found:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scan only</td>
<td>Scan the file for viruses. Deny access to the infected file, but do nothing to the infected file.</td>
</tr>
<tr>
<td>Scan and repair files</td>
<td>Scan the file for viruses. Try to repair the infected file, and deny access to any unrepairable file.</td>
</tr>
<tr>
<td>Scan and repair or delete</td>
<td>Scan the file for viruses. Try to repair the infected file, and delete any unrepairable file from archive files.</td>
</tr>
</tbody>
</table>

**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*.

4 On the toolbar, select one of the following:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Save</td>
<td>Saves your changes. You can continue to make changes in the administrative interface until you are ready to apply them.</td>
</tr>
<tr>
<td>Apply</td>
<td>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.</td>
</tr>
</tbody>
</table>

**Scheduling LiveUpdate to update virus definitions automatically**

Scheduling LiveUpdate to occur automatically at a specified time interval ensures that the Symantec Protection Engine always has the most current virus definitions. If you use multiple protection engines to support virus scanning, schedule LiveUpdate to occur at the same time for each protection engine. This scheduling ensures that all protection 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 Protection 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
protection 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™ Protection
Engine for Network Attached Storage Implementation Guide.

To schedule LiveUpdate to update virus definitions automatically

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

2 Under Views, click LiveUpdate Content.

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

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 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. On the Symantec Protection 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, select the **Enable scheduled Rapid Release** check box 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 Protection 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 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 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 7.5 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
- About preparing for installation when operating in 7-Mode
- About configuring Symantec Protection Engine to work with NetApp operating in 7-Mode
- About configuring the client NetApp storage system operating in 7-Mode
- About specifying which embedded files to scan
About software components for NetApp® Data ONTAP® 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 7.5
  Symantec Protection Engine 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” on page 42.

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 7.5 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” on page 38.

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. 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” on page 43.

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 when operating in 7-Mode” on page 46.

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” on page 38.
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 SMNP. The information that appears in the Infection Found messages that is logged to SSIM is limited as SSIM does not support some data fields.

**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.
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” on page 10.

See “System requirements to install Symantec Protection Engine on Windows” on page 12.


See “Installing Symantec Protection Engine on Windows” on page 15.

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” on page 42.

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 administrative interface. Then you can configure the RPC-specific options.

See “About configuring the RPC protocol options” on page 22.

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” on page 20.
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” on page 45.

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. On the administrative interface, in the left pane, click Configuration.
3. Under RPC Configuration, select the Automatically send AntiVirus update notifications check box.
   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 operating in 7-Mode 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**.

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. In the console on the primary navigation bar, click **Policies**.
2. In the sidebar under **Views**, click **Quarantine**.
3. In the content area under **Quarantine**, select the **Configure quarantine server** check box.
4. In the **Central quarantine server host or IP** box, type the host name or the IP address for the computer on which Symantec Central Quarantine Server is installed.
5 In the **Port** box, type the TCP/IP port number that Symantec Protection Engine uses to pass files to Symantec Central Quarantine.

6 On the toolbar, select one of the following options:

- **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 quarantine unrepairable infected files

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

2 Under **Views**, click **Scanning**.

3 In the right pane, under **Quarantine**, select the **Quarantine Threats** check box.

**Note:** To quarantine threats, you must configure the Quarantine server.

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.

---

**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 scan all files regardless of extension or type

1. On the Symantec Protection 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 Protection 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 Protection 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.

---

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.
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 `vscan extensions include` and `vscan extensions 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 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 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" on page 20.

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” on page 37.

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.

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.

### 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 scan all files regardless of extension or type**

1. On the Symantec Protection 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 Protection 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 Protection 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.
Configuring Symantec™ Protection Engine for Network Attached Storage 7.5 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 preparing for installation for clustered Data ONTAP
- About configuring Symantec Protection Engine to work with NetApp clustered Data ONTAP
- About configuring the client NetApp system running clustered Data ONTAP
- About specifying which embedded files to scan
- About configuration options
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 7.5
  Symantec Protection Engine 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 "About configuring the client NetApp system running clustered Data ONTAP" on page 61.

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 7.5 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” on page 32.

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” on page 61.

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” on page 64.

### 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” on page 57.
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. The information that appears in the Infection Found messages that is logged to SSIM is limited as SSIM does not support some data fields.

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.
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” on page 10.

See “System requirements to install Symantec Protection Engine on Windows” on page 12.


See “Installing Symantec Protection Engine on Windows” on page 15.

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” on page 61.

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.

See “About configuring the RPC protocol options” on page 22.

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” on page 20.

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” on page 63.

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. On the administrative interface, in the left pane, click Configuration.
3. Under RPC Configuration, select the Automatically send AntiVirus update notifications check box.
   
   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 system running clustered Data ONTAP when virus definitions are updated

1. On the administrative interface, in the left pane, click Configuration.
3. In the left pane, under Tasks, click Send AntiVirus Update Notification.
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. In the console on the primary navigation bar, click Policies.
2. In the sidebar under Views, click Quarantine.
3. In the content area under Quarantine, select the Configure quarantine server check box.
4. In the Central quarantine server host or IP box, type the host name or the IP address for the computer on which Symantec Central Quarantine Server is installed.
5  In the **Port** box, type the TCP/IP port number that Symantec Protection Engine uses to pass files to Symantec Central Quarantine.

6  On the toolbar, select one of the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Save</td>
<td>Saves your changes. You can continue to make changes in the administrative interface until you are ready to apply them.</td>
</tr>
<tr>
<td>Apply</td>
<td>Applies your changes. Your changes are not implemented until you apply them.</td>
</tr>
</tbody>
</table>

To quarantine unrepairable infected files

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

2  Under **Views**, click **Scanning**.

3  In the right pane, under **Quarantine**, select the **Quarantine Threats** check box.

Note: To quarantine threats, you must configure the Quarantine server.

4  On the toolbar, select one of the following:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Save</td>
<td>Saves your changes. You can continue to make changes in the administrative interface until you are ready to apply them.</td>
</tr>
<tr>
<td>Apply</td>
<td>Applies your changes. Your changes are not implemented until you apply them.</td>
</tr>
</tbody>
</table>

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 scan all files regardless of extension or type for clustered Data ONTAP

1. On the Symantec Protection 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 for clustered Data ONTAP

1. On the Symantec Protection 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:
To scan all file types except those in the file type exclusion list for clustered Data ONTAP

1. On the Symantec Protection 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.
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 7.5. 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.

See “Editing the service start-up properties” on page 20.

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.

See “Notifying the NetApp storage system operating in 7-Mode when virus definitions are updated” on page 37.

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.

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 scan all files regardless of extension or type for clustered Data ONTAP**

1. On the Symantec Protection 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 for clustered Data ONTAP

1 On the Symantec Protection 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 for clustered Data ONTAP

1 On the Symantec Protection 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:

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Save</td>
<td>Saves your changes. You can continue to make changes in the administrative interface until you are ready to apply them.</td>
</tr>
<tr>
<td>Apply</td>
<td>Applies your changes. Your changes are not implemented until you apply them.</td>
</tr>
</tbody>
</table>

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” on page 66.
- To specify the client logging information in log files
  See “Specify client information logging in log files” on page 67.
- To specify the notification threshold in case of overload
  See “Specify notification threshold is case of overload” on page 67.

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.

Table 3-1 lists the granular scan status setting for clustered Data ONTAP.
### Table 3-1  Granular scan status setting

<table>
<thead>
<tr>
<th>XPath</th>
<th>Field values</th>
<th>Default values</th>
</tr>
</thead>
<tbody>
<tr>
<td>/configuration/protocol/RPC/</td>
<td></td>
<td>true</td>
</tr>
<tr>
<td>EnableGranularScanStatus</td>
<td>■ true  Enables Symantec Protection Engine to send the granular scan status for clustered Data ONTAP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ false  Disables Symantec Protection Engine from sending the granular scan status for clustered Data ONTAP</td>
<td></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.

Table 3-2 lists the setting to log client information when a policy violation is detected.

### Table 3-2  Logging client information setting

<table>
<thead>
<tr>
<th>XPath</th>
<th>Field values</th>
<th>Default values</th>
</tr>
</thead>
<tbody>
<tr>
<td>/configuration/protocol/RPC/</td>
<td></td>
<td>false</td>
</tr>
<tr>
<td>LogClientInformation</td>
<td>■ true  Logs client information for all files</td>
<td></td>
</tr>
<tr>
<td>ForCleanFiles</td>
<td>■ false  Logs client information only when a policy violation is detected</td>
<td></td>
</tr>
</tbody>
</table>

### Specify notification threshold is 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. That is EnableGranularScanStatus = true.

Table 3-3 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/protocol/RPC/EnableServerTooBusyResponse</td>
<td><img src="true" alt="true" /> Enables Symantec Protection Engine to send a notification when the queued requests reach threshold <img src="false" alt="false" /> Disables Symantec Protection Engine from sending a notification when the queued requests reach threshold</td>
<td><img src="true" alt="true" /></td>
</tr>
</tbody>
</table>

Specify scanning via encoded path

Symantec Protection Engine, by default, enables scanning of files via their encoded paths.

Table 3-4 lists the setting to scan files via the encoded path.

Table 3-4  Scanning via the encoded path setting

<table>
<thead>
<tr>
<th>XPath</th>
<th>Field values</th>
<th>Default values</th>
</tr>
</thead>
<tbody>
<tr>
<td>/configuration/protocol/RPC/EncodedPaths</td>
<td><img src="true" alt="true" /> Enables the scanning of files via the encoded path. <img src="false" alt="false" /> Disables the scanning of files via the encoded path.</td>
<td><img src="true" alt="true" /></td>
</tr>
</tbody>
</table>
Index

A
antivirus scan policy
  configure 23

C
CIFS 32, 50
clustered Data ONTAP 50, 55
Common Internet File System 32, 50

D
Data ONTAP 7-Mode 32
Data ONTAP operating in 7-Mode 36

F
file extension exclusion list 39, 46, 58, 64
file type exclusion list 39, 46, 58, 64
file types to be scanned
  NetApp storage system 45, 64

I
ICAP
  default protocol 36, 55
infected files 34, 53
installation
  on Windows 15
  preparing for 10
Internet Content Adaptation Protocol 36, 55

N
NetApp clustered Data ONTAP
  adding Symantec Protection Engine 50
  configure 61
  system requirements 55
NetApp clustered Data ONTAP working with unresponsive protection engines 62
NetApp operating in 7-Mode working with unresponsive protection engines 44
NetApp storage system
  clustered Data ONTAP 50

NetApp storage system (continued)
  Data ONTAP operating in 7-Mode 32
  edit list 23
  editing service startup properties 20
  protocol 32, 50
  verify protection engine registration 42
NetApp storage system in 7-Mode
  activate virus scanning 43
  rollback 43
  specify file extensions 43
  vscan extensions exclude add 43
  vscan extensions exclude remove 43
  vscan extensions include add 43
  vscan extensions include remove 43
  vscan extensions include reset 43
NetApp storage system operating in 7-Mode
  cache 37, 45
  configure 42
  configuring for virus scanning 42
  overview of virus scanning 32
  system requirements 36
NetApp storage system when operating in 7-Mode
  adding Symantec Protection Engine 32
  backups 44
  quarantining infected files 38
NetApp storage system: specifying files to scan 45, 64
NetApp system running clustered Data ONTAP
  activate virus scanning 61
  backups 63
  cache 55, 63
  configuring for virus scanning 61
  overview of virus scanning 50
  rollback 61
  specify file extensions 61
  verify protection engine registration 61
  vserver vscan on-access-policy create 61
  vserver vscan on-access-policy modify 61
NetApp system running clustered Data ONTAP Data ONTAP
  quarantining infected files 57
NetApp® clustered Data ONTAP®
software components 50
NetApp® Data ONTAP® when operating in 7-Mode
software components 32
Network Appliance clustered Data ONTAP 50
Network Appliance storage system when operating in
7-Mode 32
Network File System 32, 50
NFS 32, 50

P
Preparing for installation for clustered Data ONTAP 55
Preparing for installation when operating operating in
7-Mode 36

Q
quarantine
irreparable file 33, 38, 52, 57
procedure 38, 57
RPC scan policy 38, 57
unrepairable file 34, 53
quarantining infected files
NetApp storage system when operating in
7-Mode 38
NetApp system running clustered Data ONTAP
Data ONTAP 57

R
RPC
client list 22
configure 22
handling infected files 34, 53
reconnect attempts 22
RPC client list 22
RPC protocol
NetApp storage system operating in 7-Mode 32
NetApp system running clustered Data
ONTAP 50
options 22

S
service startup properties
edit for RPC 20
NetApp storage system 20
software components
NetApp clustered Data ONTAP 50
NetApp storage system when operating in
7-Mode 32

Symantec Central Quarantine 38, 57
Symantec Protection Engine
administrative interface 36, 55
change protocol 36, 55
configure 36, 55
configuring the NetApp clustered Data ONTAP 55
configuring the NetApp storage system operating
in 7-Mode 36
installing 13
quarantine 33, 52
Rapid Release 29
scan all files 39, 46, 58, 64
Symantec Security Response
infected files 38, 57

U
unrepairable files 34, 53
unrepairable infected file 38, 57

V
virus
heuristically detected 38, 57
notification for clustered Data ONTAP 54
notification when operating in 7-Mode 35
user identification for clustered Data ONTAP 54
user identification when operating in 7-Mode 35
virus definition
automatic notification 37, 55
automatic update 27
new 38, 57
on updating 37, 55
Rapid Release definitions 29
vscan 42, 61
vscan off 43
vscan on 43
vscan options mandatory_scan 44
vscan options timeout 44
vscan reset 33
vserver vscan disable 61
vserver vscan enable 61
vserver vscan on-access-policy create 62
vserver vscan on-access-policy modify 62
vserver vscan reset 52
vserver vscan scanner-pool apply-policy 62
vserver vscan scanner-pool create 62
vserver vscan scanner-pool modify 62
vserver vscan scanner-pool servers remove 62
wildcard extension
   ???  43, 61
Windows
   installing Symantec Protection Engine  15
Windows service startup properties  36, 55