Configuring Symantec AntiVirus™ for BlueArc® Storage System
The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Documentation version: 5.2.10

Legal Notice

Copyright © 2011 Symantec Corporation. All rights reserved.

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

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

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

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

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

Symantec Technical Support maintains support centers globally. Technical Support’s primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec’s support offerings include the following:

■ A range of support options that give you the flexibility to select the right amount of service for any size organization
■ Telephone and/or Web-based support that provides rapid response and up-to-the-minute information
■ Upgrade assurance that delivers software upgrades
■ Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
■ Premium service offerings that include Account Management Services

For information about Symantec’s support offerings, you can visit our Web site at the following URL:

www.symantec.com/business/support/

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

Contacting Technical Support

Customers with a current support agreement may access Technical Support information at the following URL:

www.symantec.com/business/support/

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

■ Product release level
- Hardware information
- Available memory, disk space, and NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
  - Error messages and log files
  - Troubleshooting that was performed before contacting Symantec
  - Recent software configuration changes and network changes

Licensing and registration
If your Symantec product requires registration or a license key, access our technical support Web page at the following URL:
www.symantec.com/business/support/

Customer service
Customer service information is available at the following URL:
www.symantec.com/business/support/
Customer Service is available to assist with non-technical questions, such as the following types of issues:
- Questions regarding product licensing or serialization
- Product registration updates, such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade assurance and support contracts
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechanical presales questions
- Issues that are related to CD-ROMs or manuals
Support agreement resources

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

- Asia-Pacific and Japan: customercare_apac@symantec.com
- Europe, Middle-East, and Africa: semea@symantec.com
- North America and Latin America: supportsolutions@symantec.com
Configuring Symantec AntiVirus™ for BlueArc® Storage System

This document includes the following topics:

- About software components
- How Symantec Scan Engine works with BlueArc Storage System
- About preparing for installation
- About configuring Symantec Scan Engine
- About configuring BlueArc Storage System

**About software components**

Symantec AntiVirus for Network Attached Storage provides virus scanning and repair capabilities for BlueArc® Storage System.

Configure the following components to add antivirus scanning to BlueArc Storage System:

- Symantec Scan Engine, which provides the virus scanning and repair services. For more information, see the *Symantec Scan Engine Implementation Guide*.
- For BlueArc Storage System some options are configured directly on the NAS Server. No additional code is necessary to connect Symantec Scan Engine to the NAS Server.

See “About configuring BlueArc Storage System” on page 23.
How Symantec Scan Engine works with BlueArc Storage System

Symantec AntiVirus for Network Attached Storage provides virus scanning and repair capabilities for BlueArc Storage System storage appliances that have firmware version 7.0, 8.0, or 10.0.

Symantec Scan Engine must be installed on a computer that is running Windows 2000 Server/Windows 2003 Server/Windows 2008 Server. It must be located in the same domain as the NAS Server for which it provides scanning and repair services. Symantec Scan Engine uses the RPC protocol to interface with BlueArc Storage System storage appliances.

On the NAS Server, you can enable virus scanning individually for each Enterprise Virtual Server (EVS). An EVS is a virtual NAS system that consists of CIFS shares with individual IP addresses. A single Symantec Scan Engine can support multiple EVSs. Hence, represent each EVS as an RPC client through the Symantec Scan Engine administrative interface. You can use multiple scan engines to support one or more EVSs for sites with larger scan volumes. Load balancing is handled through the NAS Server’s administrative interface to achieve high availability and performance scaling.

Virus scanning on BlueArc Storage System is available only for those files that are requested through the Common Internet File System (CIFS).

What happens when a file is scanned

The NAS Server submits files to Symantec Scan Engine for scanning on both read and write. That is, files are scanned when they are accessed from storage (read) and if they are changed on the NAS Server (write).

When a user tries to access a file, the NAS Server passes the file path to Symantec Scan Engine for scanning. After the file is opened and scanned, Symantec Scan Engine indicates the scanning results to the NAS Server. The scan engine returns the repaired file based on a configurable virus scan policy if a file is infected and can be repaired.

The NAS Server passes the clean files to the requesting user after it received 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. You can configure Symantec Scan Engine to quarantine these unrepairable files.

After a file has been scanned and declared clean, the scanned state information is stored in its metadata on disk. It avoids redundant scans of those files that have
already been scanned. These files will not be scanned again unless they are modified or the administrator requests a full scan of the files from the NAS Server's administrative interface.

See “About executing a full file system scan” on page 25.

About connecting to Symantec Scan Engine

Symantec Scan Engine monitors the connection with each EVS by checking the connection at a configured time interval. The scan engine tries to reconnect if it determines that the connection is not active. (You can configure the number of times that the scan engine tries to re-establish the connection.)

About limiting scanning by file type

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

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

You can control the files that are initially submitted to the scan engine by BlueArc Storage System for scanning.

The NAS Server lets you specify by file extension the files that are to be passed to Symantec Scan Engine for scanning. You configure the file types that you want to submit for scanning through the NAS Server interface in accordance with the product documentation.

See “About specifying the file extensions to be scanned on the NAS Server” on page 25.

You can control the files that are embedded in archival file formats (for example, .zip or .lzh files) that are to be scanned by Symantec Scan Engine.

The file extension exclusion list and the file type exclusion lists let you specify the file types and the file extensions that you do not want to scan. The file extensions exclusion list and the file type exclusion list achieve this purpose. You can also scan all file types regardless of extension. You configure which embedded files are scanned through the Symantec Scan Engine administrative interface.

See “Specify which embedded files to scan” on page 19.
About handling infected files

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

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

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

See “About quarantining unrepairable infected files” on page 17.

About user identification and notification when a virus is found

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

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

**Note:** Symantec Scan Engine can obtain only the information that is made available by the NAS Server. 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 NAS Server is omitted from the log messages and from the user notification window.

You also can configure Symantec Scan Engine to notify the requesting user that the retrieval of a file failed because a virus was found. The notification message only appears if the user uses a Windows computer.

The notification message includes the following:

- Date and time of the event
- File name of the infected file
About preparing for installation

BlueArc Storage System storage appliance must support a firmware version of 7.0, 8.0, or 10.0 to interface with Symantec Scan Engine. As a prerequisite, ensure that each NAS Server for which the scan engine is to provide scanning and repair services meets this requirement.

To use RPC, Symantec Scan Engine must be installed on a computer that is running Windows 2000 Server/Windows 2003 Server/Windows 2008 Server. The computer on which you plan to install Symantec Scan Engine must meet the system requirements that are listed in the Symantec Scan Engine Implementation Guide.

After you install Symantec Scan Engine, configure the NAS Server to work with the scan engine.

See “About configuring BlueArc Storage System” on page 23.

About configuring Symantec Scan Engine

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

See “About configuring RPC protocol options” on page 12.

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

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

If you change the protocol setting to RPC through the Symantec Scan Engine administrative interface, you need to change the service startup properties to identify an account that has the following appropriate permissions:

- The account must have local administrator permissions on the computer that has the scan engine.
- The user account must have Backup Operator privileges or above on the NAS Server.
  
  For more information on how to set up a shared account with local group backup operator privileges on the NAS Server, see the appropriate product documentation.

You must change the service startup properties if the list of NAS Servers is edited as well.

To edit the service startup properties

1. In the Windows 2000/2003/2008 Control Panel, click **Administrative Tools**.
2. Click **Services**.
3. In the list of services, right-click **Symantec Scan Engine**, and then click **Properties**.
4. In the Properties dialog box, on the Log On tab, click **This Account**.
5. Type the account name and password for the user account that has local administrator rights on the computer that has the scan engine. This account should also have Backup Operator privileges or above on the NAS Server.

  Use the following format for the account name:
  
  domain\username

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

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

About configuring RPC protocol options

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

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

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| RPC client list                             | A single Symantec Scan Engine can support one or more EVSs. Each EVS must be located in the same domain as Symantec Scan Engine. You must provide the IP address of each EVS.  

**Note:** Multiple scan engines can support a single EVS. Configure the multiple scan engines through the BlueArc Storage System interface.  |
| Check RPC connection every __ seconds       | Symantec Scan Engine maintains a connection with the EVS on the NAS Server. Symantec Scan Engine can be configured to check the connection with the EVS at a prescribed interval to ensure that the connection is active. The default value is 20 seconds. |
| Maximum number of reconnect attempts        | You can configure Symantec Scan Engine to make a specified number of tries to re-establish a lost connection with the EVS. By default, Symantec Scan Engine is configured to try to reconnect with the EVS indefinitely. 

**Note:** Do not set a maximum number of reconnect attempts if the scan engine provides scanning for multiple Enterprise Virtual Servers. Use the default setting. |
Table 1-1  Protocol-specific options for RPC (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Antivirus scan policy</td>
<td>You can configure Symantec Scan Engine to do one of the following when an infected file is found:</td>
</tr>
<tr>
<td>■ Scan only: Deny access to the infected</td>
<td></td>
</tr>
<tr>
<td>file, but do nothing to the infected</td>
<td></td>
</tr>
<tr>
<td>file.</td>
<td></td>
</tr>
<tr>
<td>■ Scan and repair files: Try to repair the</td>
<td></td>
</tr>
<tr>
<td>infected file, and deny access to any</td>
<td></td>
</tr>
<tr>
<td>unrepairable file.</td>
<td></td>
</tr>
<tr>
<td>■ Scan and repair or delete: Try to repair</td>
<td></td>
</tr>
<tr>
<td>the infected file, and delete any</td>
<td></td>
</tr>
<tr>
<td>unreparable file.</td>
<td></td>
</tr>
<tr>
<td>Note: You must select Scan and repair or</td>
<td>曜 you plan to quarantine the infected files that cannot be repaired. For more information, see the Symantec Scan Engine Implementation Guide.</td>
</tr>
<tr>
<td>delete if you plan to quarantine the</td>
<td></td>
</tr>
<tr>
<td>infected files that cannot be repaired.</td>
<td></td>
</tr>
<tr>
<td>Automatically send antivirus update</td>
<td>You can configure Symantec Scan Engine to automatically notify BlueArc Storage System when new virus definitions are used.</td>
</tr>
<tr>
<td>notifications</td>
<td></td>
</tr>
</tbody>
</table>

How to configure RPC protocol options

To configure RPC, do the following:

■ Provide an IP address for each EVS for which Symantec Scan Engine should provide scanning services. You can add or delete Enterprise Virtual Servers from this list at any time.

■ Configure the additional RPC-specific options.

To edit the list of NAS Servers

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

2 Under Views, click Protocol.

3 In the right pane, under Select Communication Protocol, click RPC.

   The configuration settings are displayed for the selected protocol.

4 In the Manual Restart Required dialog box, click OK.
To add an EVS to the list of RPC clients, type the IP address of the EVS for which Symantec Scan Engine should provide scanning services. Type one entry per line.

To delete an EVS from the list of RPC clients, select and delete the IP address of the EVS.

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 EVS.

**To configure additional RPC-specific options**

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

2. Under Views, click **Protocol**.

3. Under RPC Configuration, in the Check RPC connection every box, type how frequently Symantec Scan Engine checks the RPC connection with the EVS to ensure that the connection is active.
   - The default interval is 20 seconds.

4. In the Maximum number of reconnect attempts box, type the maximum number of tries that the Symantec Scan Engine should undertake to reestablish a lost connection with the EVS.
   - The default setting is 0. Symantec Scan Engine tries indefinitely to reestablish a connection. Use the default setting if the scan engine provides scanning for multiple enterprise virtual servers.
5. In the Antivirus scan policy list, select how you want Symantec Scan Engine to handle infected files.

   The default setting is Scan and repair or delete.

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

<table>
<thead>
<tr>
<th>Action</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 EVS.</td>
</tr>
</tbody>
</table>

### Notifying a requesting user that a virus was found

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

The notification message includes the following information:

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

To notify a requesting user that a virus was found

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

User notification is disabled by default.

4. On the toolbar, select one of the following:
   - Save: Saves your changes. You can continue to make changes in the administrative interface until you are ready to apply them.
   - Apply: Applies your changes. Your changes are not implemented until you apply them. You must perform a manual restart for the changes to take place.

About quarantining unrepairable infected files

You can quarantine unrepairable infected files when you use the RPC protocol. To use the quarantine feature, Symantec Central Quarantine must be installed separately on a computer that runs Windows 2000 Server/Windows 2003 Server/Windows 2008 Server. Symantec Central Quarantine is included on the Symantec Scan Engine distribution CD along with supporting documentation.

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

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 NAS Server. Access to the infected file is denied.
See “About configuring RPC protocol options” on page 12.

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

To quarantine unrepairable infected files

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

2. Under Views, click Scanning.

3. In the right pane, under Quarantine, check Quarantine files.

4. In the Central server quarantine host or IP box, type the host name or the IP address for the computer on which Symantec Central Quarantine is installed.

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

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

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

   - **Save**
     - Saves your changes.
     - You can continue to make changes in the administrative interface until you are ready to apply them.

   - **Apply**
     - Applies your changes.
     - Your changes are not implemented until you apply them.

---

### Specifying which embedded files to scan

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

When the scan engine receives an archive file (for example, a .zip or .lzh file) that contains embedded files, it must break down the archive file and scan each embedded file. You can control, through the scan engine administrative interface, which embedded files are scanned by using a file extension and file type exclusion list. You can also scan all files regardless of extension.
Symantec Scan Engine is configured by default to scan all files. The file type and file extension exclusion lists are prepopulated with the file types that are unlikely to contain viruses, but you can edit this list.

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

### Specify which embedded files to scan

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

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

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

   - **Save**
     - Saves your changes.
     - You can continue to make changes in the administrative interface until you are ready to apply them.

   - **Apply**
     - Applies your changes.
     - Your changes are not implemented until you apply them.

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

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

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

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

6 To restore the default file extension exclude list, in the left pane, under Tasks, click **Reset Default List**. This option restores the default file-type exclude list and the file-extension exclude list.

7 On the toolbar, select one of the following:

<table>
<thead>
<tr>
<th></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 scan all file types except those in the file type exclusion list**

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

2 Under Views, click **Scanning**.

3 In the right pane, under Files to Scan, click **Scan all files except those in the extension or type exclude lists**. When you activate this option, both the file type exclude list and the file extension exclude list are activated automatically.

4 Type each file type that you want to add to the list on a separate line. To include all subtypes for a file type, use the wildcard character /*. For more information on how to write the file types, see the **Symantec Scan Engine Implementation Guide**.

5 To remove a file type from the list, select it and delete it from the File type exclude list.
6 To restore the default file type exclude list, in the left pane, under Tasks, click **Reset Default List**.

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

7 On the toolbar, select one of the following:

- **Save**
  Saves your changes.
  You can continue to make changes in the administrative interface until you are ready to apply them.

- **Apply**
  Applies your changes.
  Your changes are not implemented until you apply them.

---

**Scheduling LiveUpdate to update virus definitions automatically**

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

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

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

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

**To schedule LiveUpdate to update virus definitions automatically**

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

2 Under Views, click **LiveUpdate Content**.
3 In the right pane, under LiveUpdate Content, check **Enable scheduled LiveUpdate**.

   This option is enabled by default.

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

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

5 On the toolbar, select one of the following:

   - **Save** Saves your changes.
     
     You can continue to make changes in the administrative interface until you are ready to apply them.

   - **Apply** Applies your changes.
     
     Your changes are not implemented until you apply them.

### Configuring Rapid Release updates to occur automatically

You can configure Symantec Scan Engine to obtain uncertified definition updates with Rapid Release. You can configure Symantec Scan Engine to retrieve Rapid Release definitions every 5 minutes to every 120 minutes.

Rapid Release definitions are created when a new threat is discovered. Rapid Release definitions undergo basic quality assurance tests by Symantec Security Response. However, they do not undergo the intense testing that is required for a LiveUpdate release. Symantec updates Rapid Release definitions as needed to respond to high-level outbreaks.

**Warning:** Rapid Release definitions do not undergo the same rigorous quality assurance tests as LiveUpdate and Intelligent Updater definitions. Symantec encourages users to rely on the full quality-assurance-tested definitions whenever possible. Ensure that you deploy Rapid Release definitions to a test environment before you install them on your network.

If you use a proxy or firewall that blocks FTP communications, the Rapid Release feature does not function. Your environment must allow FTP traffic for the FTP session to succeed.
You can schedule Rapid Release updates to occur automatically at a specified time interval to ensure that Symantec Scan Engine always has the most current definitions. Scheduled Rapid Release updates are disabled by default.

**To configure Rapid Release updates to occur automatically**

1. On the Symantec Scan Engine administrative interface, in the left pane, click **System**.
2. Under Views, click **Rapid Release Content**.
3. In the content area under Rapid Release Content, check **Enable scheduled Rapid Release** to enable automatic downloads of Rapid Release definitions. This option is disabled by default.
4. In the Rapid Release interval box, to specify the interval between which you want Symantec Scan Engine to download Rapid Release definitions, do any of the following steps:
   - Type the interval.
   - Click the up arrow or down arrow to select the interval.
   You can select any number between 5 minutes and 120 minutes. The default value is 30 minutes.
5. On the toolbar, select one of the following:
   - **Save** Saves your changes.
     You can continue to make changes in the administrative interface until you are ready to apply them.
   - **Apply** Applies your changes.
     Your changes are not implemented until you apply them.

**About configuring BlueArc Storage System**

After you configure Symantec Scan Engine to use RPC as the communication protocol, configure the client Enterprise Virtual Servers (EVSs) to work with Symantec Scan Engine.

BlueArc Storage System EVS clients must be running a firmware version 7.0, 8.0, or 10.0 to interface with the Symantec Scan Engine.
Each EVS should be installed and configured in accordance with the accompanying product documentation. Each EVS should be functional before you initiate virus scanning using Symantec Scan Engine.

You must set up a shared account with backup operator privileges on the NAS Server before you configure virus scanning on the NAS Server. Ensure that Symantec Scan Engine service runs with this shared account as well.

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

For more information on how to set up a shared account with local group backup operator privileges on the NAS Server, see the appropriate NAS Server documentation.

The main virus scanning parameters that you should configure can be found in the “Virus Scanning” page under the “Data Protection” section of the NAS Servers administrative interface. You will also need to enable virus scanning on each individual share that you require scans to be performed on.

About verifying that the scan engine is registered with the NAS Server

You can verify that the scan engine is registered with the NAS Server after you install Symantec Scan Engine. Registration is automatic if you have provided the correct information to Symantec Scan Engine for contacting the EVS. Registration occurs when Symantec Scan Engine connects to the EVS. The “Registered Virus Scanners” field in the NAS Server’s administrative interface contains the names of the registered scan engines. Ensure that at least one registered scan engine is present to be assured of virus protection for each EVS.

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

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

About enabling virus scanning on CIFS shares

Once the scan engine has been registered and configured, it is necessary to enable virus scanning on each individual CIFS share. This should be done via the NAS Servers administrative interface, by going to the “CIFS Share” page under the “File Services” section, and selecting the details of each share in turn and making sure that the “Enable Virus Scanning” check box is checked. If virus scanning is not enabled on a CIFS share, access to the files will be unrestricted.
About activating virus scanning

You can activate and deactivate virus scanning for each EVS. Select the EVS for which you want to activate scanning from the “EVS” drop-down box. Check “Enable Virus Scanning” in the NAS Server’s administrative interface to activate virus scanning. Uncheck “Enable Virus Scanning” to deactivate virus scanning.

For more information, see the appropriate NAS Server documentation.

About specifying the file extensions to be scanned on the NAS Server

Configure the list of extensions on BlueArc Storage System to contain only the file extensions that you want to scan. This list lets you control the file types that are passed to the Symantec Scan Engine for scanning. You can configure file extensions using the extensions inclusion list seen in the “File types to scan” field.

A default list of extensions to be submitted for virus scanning is included with the NAS Server. You can modify the inclusion list by adding or removing extensions.

To rollback to the default inclusion list, click “Reset Defaults.” To scan all file types irrespective of extensions, check “Scan All File Types.” 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 NAS Server documentation.

About executing a full file system scan

You can flag all files for a re-scan if there are new updated virus definition files on Symantec Scan Engine. Click “Request Full Scan” in the NAS Server’s administrative interface to ensure that all file types listed in the inclusion list are marked for scan. The scan on a file occurs the next time any user accesses the file.

About working with unavailable scan engines

BlueArc Storage System is configured to deny access to files if virus scanning is enabled and the scan engines are not available. Ensure that more than one scan engine is configured for the CIFS shares on the NAS Server so that maximum accessibility of data is guaranteed.

You can deactivate virus scanning until the scan engines are available again so that file access is still available. BlueArc Storage System keeps a track of all files
that are not scanned in this duration. As soon as virus scanning is activated, the files that were created/modified in the duration are scanned without fail.

For more information, see the appropriate NAS Server documentation.

About working with unresponsive scan engines

When large or complex files are scanned (for example, container files with multiple embedded files or files that contain polymorphic or macro viruses), the scan engine can become unresponsive. Clients cannot, temporarily, access the files. The user can eventually access the file when the scanning is complete and if the file is deemed clean by the scan engine.

For more information, see the appropriate NAS Server documentation.
antivirus scan policy configure 14

BlueArc Storage System
activate virus scanning 25
add antivirus scanning 7
antivirus scan policy 12
automatically send antivirus update notifications 12
check RPC connection 12
configuring for virus scanning 23
configuring scan engine 11
connecting to Symantec Scan Engine 9
edit NAS Server list 14
editing service startup properties 12
enable virus scanning 25
file scanning 8
file type scanning 9
firmware version 11, 23
full file system scan 25
handling infected files 10
maximum number of reconnect attempts 12
overview of virus scanning 8
protocol 8
quarantining infected files 17
registered virus scanners 24
reset defaults 25
RPC client list 12
scan all file types 25
software components 7
specify file extensions 25
specifying files to scan 18
system requirements 11
unavailable scan engines 25
unresponsive scan engines 26
user notification of infection found 10, 16
verify scan engine registration 24

CIFS shares 24

enable virus scanning 24

file extension exclusion list 19
file type exclusion list 19
file types to be scanned
BlueArc Storage System 18

notification message
event security level 16
information contained 16
scan policy 16
virus name 16
notification of infection found
BlueArc Storage System 10, 16

quarantine
procedure 17
RPC scan policy 17
unrepairable file 17
quarantining infected files
BlueArc Storage System 17

Rapid Release
automatic update 22
RPC
configure 14
RPC options
antivirus scan policy 12
automatically send antivirus update notifications 12
check RPC connection 12
RPC options *(continued)*
  maximum number of reconnect attempts 12
  RPC client list 12
RPC protocol
  options 12

S
service startup properties
  BlueArc Storage System 12
  edit for RPC 12
software components
  BlueArc Storage System 7
Symantec Central Quarantine 17
Symantec Scan Engine
  enable Windows messenger logging 16
  LiveUpdate 21
  scan all files 19
Symantec Security Response
  infected files 17

V
virus
  definition date 10
  heuristically detected 17
  notification 10
  user identification 10
virus definition
  automatic update 21
  new 17
  Rapid Release definitions 22