Configuring Symantec AntiVirus™ for HP IBRIX X9000 Storage System
Configuring Symantec AntiVirus™ for HP IBRIX X9000 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 © 2012 Symantec Corporation. All rights reserved.

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

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

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

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

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

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

Symantec’s support offerings include the following:

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

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

www.symantec.com/business/support/

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

Contacting Technical Support

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

www.symantec.com/business/support/

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

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

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

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

Customer service
Customer service information is available at the following URL:
www.symantec.com/business/support/
Customer Service is available to assist with non-technical questions, such as the following types of issues:
  Questions regarding product licensing or serialization
  Product registration updates, such as address or name changes
  General product information (features, language availability, local dealers)
  Latest information about product updates and upgrades
  Information about upgrade assurance and support contracts
  Information about the Symantec Buying Programs
  Advice about Symantec's technical support options
  Nontechnical presales questions
  Issues that are related to CD-ROMs, 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
Configuring Symantec AntiVirus™ for HP IBRIX X9000 Storage System

This document includes the following topics:

- About software components
- How Symantec Scan Engine works with the HP IBRIX X9000 Storage System
- About preparing for installation
- About configuring Symantec Scan Engine
- About configuring the HP IBRIX X9000 Storage System
- Recommendations while integrating multiple scan engines

About software components

Symantec AntiVirus for Network Attached Storage provides virus scanning for HP IBRIX X9000 Storage System.

Configure the following components to add antivirus scanning to the HP IBRIX X9000 Storage System:

- Symantec Scan Engine
  Provides the virus scanning and repair services. For more information, see the Symantec Scan Engine Implementation Guide.

- HP IBRIX X9000 Storage System
  Some options are configured directly on the NAS device. No additional code is necessary to connect Symantec Scan Engine to the NAS device.
How Symantec Scan Engine works with the HP IBRIX X9000 Storage System

Symantec AntiVirus for Network Attached Storage provides virus scanning for the HP network attached storage devices that support HP IBRIX X9000 Storage 6.1 and later.

The Internet Content Adaptation Protocol (ICAP) is used to communicate with Symantec Scan Engine. In a typical HP NAS environment, a minimum of two scan engines are recommended to handle scan volume. A maximum of 50 scan engines can be supported per cluster. The ibravscand service handles load balance across multiple scan engines automatically.

How are files scanned

The HP IBRIX X9000 Storage System is configured to scan a file on Read access. The system currently provides configuration to control scanning during CIFS access. Configuration control for CIFS provides option for antivirus scan to be done on Open, Close, or both Open and Close. There is an exception for scan on Close or scan on Open. Scan on Close and scan on Open can only be configured for CIFS at present. Remaining protocols like FTP/NFS/HTTP do a scan on Read by default.

The HP IBRIX X9000 Storage System is also configured to scan when the virus definitions on the Scan Engine have changed.

The X9000 opens a connection with the Symantec Scan Engine to scan a file over which the file data is passed. The NAS device then passes the file to the scan engine for scanning. When scanning is complete, the NAS device closes the connection with the scan engine.

The Symantec Scan Engine indicates the scanning results to the NAS device after a file is scanned. Access is denied by default for infected files and corresponding file is quarantined even when the repaired copy is returned by the Symantec Scan Engine. After the NAS device receives the scanning results, the file is handled in the following way: Only clean files are passed to the requesting user. If the file is infected, the user is denied access to the file, and the infected file is quarantined. User needs to clean the infected file manually.

How caching works

The NAS device caches scanning results for each clean file. The cached information includes the date and revision number of the virus definitions that were used to perform the scan. So, if a second user requests access to a file that has already
been scanned and if the virus definitions have not changed, a redundant scan is avoided.

The cache is purged only when a stored file is changed.

**About specifying which file types are scanned**

To specify the file types to be scanned for viruses, configure settings on both the HP IBRIX X9000 Storage System and Symantec Scan Engine.

**About specifying file types on the NAS device**

Based on file extensions and file size, the NAS device determines, initially, whether it should pass a file to Symantec Scan Engine for scanning. You configure which files are passed to Symantec Scan Engine for scanning when you set up the HP IBRIX X9000 Storage System.

You can control which files are scanned by using the exclusion list, or you can scan all files regardless of extension. Configure the HP IBRIX X9000 Storage System to pass all file types to the scan engine except those that are contained in the exclusion list. The exclusion list can include extensions for those file types that are not likely to contain viruses and can be excluded from scanning. You can also exclude all files larger than the specified size (in MB) from scanning.

See “About configuring virus scanning on the HP IBRIX X9000 Storage System” on page 20.

**About specifying file types on Symantec Scan Engine**

You can configure Symantec Scan Engine so that selected file types and file extensions are excluded from scanning. The setting on Symantec Scan Engine is as important as the NAS device settings. This setting on the scan engine determines which files to scan upon receiving a file from the NAS device. The scanned files are those contained in archive or container file formats. You can control which embedded files are scanned by using the file type and extension exclusion list, or you can scan all files regardless of extension.

---

**Note:** Exclusion lists ensure that all file types are not scanned; therefore, new types of viruses might not be detected. Scanning all files regardless of extension and type is the most secure setting, but it imposes the heaviest demand on resources. During virus outbreaks, you might want to scan all files even if you normally control the file types that are scanned with the exclusion list.

See “Specifying which file types to scan” on page 14.
For more information, see the Symantec Scan Engine Implementation Guide.

### About specifying the scan policy

You configure the scan policy through the Symantec Scan Engine administrative interface. When an infected file is found, the scan engine can do any of the following:

<table>
<thead>
<tr>
<th>Policy</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scan Only</td>
<td>Scan files for viruses, but do nothing to infected files.</td>
</tr>
<tr>
<td>Scan and delete</td>
<td>Scan files for viruses, and delete any infected files that are embedded in archive or container files without trying to repair.</td>
</tr>
<tr>
<td>Scan and repair files</td>
<td>Try to repair the infected file, and deny access to any irreparable file.</td>
</tr>
<tr>
<td>Scan and repair or delete</td>
<td>Try to repair the infected file, and delete any irreparable file. You cannot configure this policy on HP IBRIX X9000 Storage System.</td>
</tr>
</tbody>
</table>

**Note:** We recommend that you set the policy to Scan Only on the Symantec Scan Engine for HP IBRIX X9000 Storage System. Irrespective of the policy set on the Symantec Scan Engine, HP IBRIX X9000 Storage System does not take any other action and quarantines the infected file. Repair or delete policy is not configurable on the HP IBRIX X9000 Storage System.

### About handling infected files on the NAS device

When an infected file is found, the NAS device does not delete the file, even though the scan engine tells it to. Instead, the NAS device quarantines the file and denies any access to the file. You can use the quarantine utility on the NAS device to manage infected files and perform actions like move, delete, or list the infected files. The quarantined files can be deleted or removed from quarantine by using the command-line interface in the HP IBRIX X9000 Storage System.

For more information, see the appropriate HP IBRIX X9000 Storage System documentation.
About preparing for installation

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 have installed the Symantec Scan Engine, configure the virus scanning functionality on the HP IBRIX X9000 Storage System.

About configuring Symantec Scan Engine

You must configure several settings on each Symantec Scan Engine that is used to support scanning for HP IBRIX X9000 Storage System.

Note: If you use multiple scan engines to support scanning, the configuration settings on each scan engine must be identical. LiveUpdate should be scheduled to occur at the same time on all scan engines so that virus definitions are consistent at all times.

The scan engine must be configured to use ICAP as the communication protocol. ICAP is the default protocol at installation. After you have selected ICAP, you can configure ICAP-specific options.

See “About configuring the HP IBRIX X9000 Storage System” on page 19.

Configuring ICAP-specific options

You can configure several settings that are specific to the ICAP protocol through the Symantec Scan Engine administrative interface. You can also change the protocol through the administrative interface if Symantec Scan Engine has already been configured to use another protocol. However, you must manually restart the Symantec Scan Engine.

For more information about accessing the administrative interface, see the Symantec Scan Engine Implementation Guide.

Table 1-1 describes the protocol-specific options for ICAP.
Table 1-1  Protocol-specific options for ICAP

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bind address</td>
<td>Symantec Scan Engine detects all of the available IP addresses that are installed on the host. By default, Symantec Scan Engine accepts scanning requests on (binds to) all of the scanning IP addresses that it detects. You can configure up to 64 IP addresses as scanning IP addresses. You can specify whether you want Symantec Scan Engine to bind to all of the IP addresses that it detects, or you can restrict access to one or more interfaces. If you do not specify at least one IP address, Symantec Scan Engine binds to all of the scanning IP addresses that it detects. If Symantec Scan Engine fails to bind to any of the selected IP addresses, an event is written to the log as a critical error. Even if Symantec Scan Engine is unable to bind to any IP address, you can access the console. However, scanning functionality is unavailable. <strong>Note:</strong> You can use 127.0.0.1 (the loopback interface) to let only the clients that are running on the same computer connect to Symantec Scan Engine.</td>
</tr>
<tr>
<td>Port number</td>
<td>The port number must be exclusive to Symantec Scan Engine. For ICAP, the default port number is 1344. If you change the port number, use a number greater than 1024 that is not in use by any other program or service.</td>
</tr>
</tbody>
</table>
Table 1-1  Protocol-specific options for ICAP (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scan policy</td>
<td>When an infected file is found, Symantec Scan Engine can do any of the following:</td>
</tr>
</tbody>
</table>
|                       |  ■ Scan only
Scan files for viruses, but do nothing to infected files.                                                                                                                                                 |
|                       |  ■ Scan and delete
Scan files for viruses, and delete any infected files that are embedded in archive or container files without trying to repair.                                                                              |
|                       |  ■ Scan and repair files
Try to repair infected files, but do nothing to irreparable files (that is, do not delete the files from archive or container files).                                                                          |
|                       |  ■ Scan and repair or delete
Try to repair infected files, and delete irreparable files from archive or container files.                                                                                                                  |

To configure ICAP-specific options

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 **ICAP**.

The configuration settings are displayed for the selected protocol. If you change the protocol setting from RPC to ICAP through the Symantec Scan Engine administrative interface, you must manually stop and start the service.

4  Under **ICAP Configuration**, in the Bind address box, select the scanning IP addresses that you want to bind to Symantec Scan Engine.

Check Select All to select every IP address in the Bind address table. By default, Symantec Scan Engine binds to all interfaces.

5  In the Port number box, type the TCP/IP port number that the \texttt{ibravscand} service uses to pass files to Symantec Scan Engine for scanning. The default setting for ICAP is port 1344.
6 In the **Scan policy** list, select how you want Symantec Scan Engine to handle infected files. The default setting is Scan and repair or delete. HP IBRIX X9000 Storage System recommends the setting Scan Only.

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>

### Specifying which file types to scan

The settings on Symantec Scan Engine must be configured to specify the types of files to be scanned for viruses. The scan policy on the scan engine determines which files it should scan from the NAS device. The scanned files are those contained in archive or container file formats.

You can control which embedded files are scanned by using an extension or type exclusion list, or you can scan all files regardless of extension and type. A prepopulated extension and type exclusion list exists that you can modify. Symantec Scan Engine is configured by default to scan all files.

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

**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**. When you enable this option, both the file extension exclude list and the file type exclude list are 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>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.</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 enable 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 /*.

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:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Save</strong></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><strong>Apply</strong></td>
<td>Applies your changes. Your changes are not implemented until you apply them.</td>
</tr>
</tbody>
</table>

---

**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:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Save</strong></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><strong>Apply</strong></td>
<td>Applies your changes. Your changes are not implemented until you apply them.</td>
</tr>
</tbody>
</table>

---

**About specifying container handling limits**

File attachments that consist of container files can overload the system and cause denial-of-service attacks. They can be overly large, contain large numbers of embedded, compressed files, or be designed to maliciously use resources and degrade performance. Symantec Scan Engine can be configured to impose limits on how container files are handled. This reduces the network’s exposure to denial-of-service attacks.
You can specify the following limits for handling container files:

- The maximum amount of time, in seconds, that is spent decomposing a container file and its contents. This setting does not apply to .hqx or .amg files.
- The maximum file size, in megabytes, for the individual files that are in a container file.
- The maximum number of nested levels to decompose for scanning.
- The maximum number of bytes that are read when determining whether a file is MIME-encoded.

You can specify whether to allow or deny access to the file if any of these specified limits is met or exceeded.

Symantec Scan Engine blocks container files based on their type, because only certain file types contain virus or malicious code. You can configure Symantec Scan Engine to block partial container files, malformed container files, and encrypted container files as well.

For more information on container handling limits, see the Symantec ScanEngine Implementation Guide.

**Scheduling LiveUpdate to update virus definitions automatically**

Scheduling LiveUpdate to occur automatically at a specified time interval ensures that Symantec Scan Engine always has the most current virus definitions. Schedule LiveUpdate to occur at the same time for each scan engine if you use multiple scan engines to support virus scanning. 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 HP IBRIX X9000 Storage System.

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

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

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

This option is enabled by default.

In the LiveUpdate interval list, choose an interval.

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

On the toolbar, select one of the following:

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

### Configuring Rapid Release updates to occur automatically

You can configure Symantec Scan Engine to obtain uncertified definition updates with Rapid Release. You can configure Symantec Scan Engine to retrieve Rapid Release definitions every 5 minutes to every 120 minutes. Rapid Release definitions are created when a new threat is discovered.

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

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

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

**Configuring Rapid Release updates to occur automatically**

1. On the Symantec Scan Engine administrative interface, in the left pane, click **System**.
2. Under **Views**, click **Rapid Release Content**.
3. In the content area under **Rapid Release Content**, check **Enable scheduled Rapid Release** to enable automatic downloads of Rapid Release definitions. This option is disabled by default.
4. In the Rapid Release interval box, to specify the interval between which you want Symantec Scan Engine to download Rapid Release definitions, do any of the following steps:
   - Type the interval.
   - Click the up arrow or down arrow to select the interval.

   You can select any number between 5 minutes and 120 minutes. The default value is 30 minutes.
5. On the toolbar, select one of the following:

   - **Save** saves your changes.
   - You can continue to make changes in the administrative interface until you are ready to apply them.
   - **Apply** applies your changes. Your changes are not implemented until you apply them.

---

**About configuring the HP IBRIX X9000 Storage System**

You must configure the virus scan functionality in accordance with the HP IBRIX X9000 Storage System documentation. The NAS device for which you provide virus scanning must be HP IBRIX X9000 Storage System 6.1 or later network attached storage device.

For more information, see the appropriate HP IBRIX X9000 Storage System documentation.
About registering Symantec Scan Engine

In a typical environment, a minimum of two scan engines is required to handle scan volume per cluster. Having one scan engine can cause denial-of-file access, in which case the engine does not respond. A maximum of 50 scan engines can be supported per cluster. The ibravscand service handles load balancing across multiple scan engines automatically.

You register Symantec Scan Engine through Cluster Configuration > Antivirus > Virus Scan Engines. You must provide the IP address and the port number for each scan engine that is used for scanning. The port number must match the port number that was selected during the installation of Symantec Scan Engine.

About configuring virus scanning on the HP IBRIX X9000 Storage System

You configure the virus scan functionality through GUI or the CLI. On the GUI, select Cluster Configuration from the Navigator, and then select Antivirus from the lower Navigator. The Antivirus Settings panel displays the current configuration.

**Note:** Please note that the Scan Engine is not configurable per file system. Once the Scan Engine is configured on a X9000 System, the same applies to all X9000 file systems.

Table 1-2 describes the settings that you should configure for virus scan functionality.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Anti Virus</td>
<td>On the GUI, select AV Enable/Disable File Systems from the lower Navigator to open the AV Enable Disable panel, which lists the file systems in the cluster. Select the file system to be enabled, click Enable, and confirm the operation. To disable Antivirus, click Disable.</td>
</tr>
</tbody>
</table>
Table 1-2  Virus scan settings (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scan Engine IP address and port number</td>
<td>Type the IP address and the port number of each scan engine to be used for scanning. Ensure that the entered port number matches the one used while installing the scan engine. Each X9000 file system cluster can support up to 50 scan engines.</td>
</tr>
<tr>
<td>Max File Scan Size</td>
<td>Specify an upper limit for the size of files to be scanned. Excludes all files larger than the specified size (in MB) from scanning. Note: Allowing access to files that have not been scanned can make your network vulnerable to virus attacks.</td>
</tr>
<tr>
<td>Exclude File Extensions</td>
<td>Specify the file types to exclude from scanning. You can use either exclusion list, or you can scan all files regardless of extension or size by selecting No Rule. This setting is similar to the Files to scan setting on Symantec Scan Engine. You must configure this setting on both the X9000 file system and Symantec Scan Engine.</td>
</tr>
</tbody>
</table>

If one scan engine does not respond, the NAS device requests virus scanning for a given file from other registered scan engines. If none respond, then file access is allowed by default. You can configure the HP IBRIX X9000 system to change the default settings to Deny Access.

**Recommendations while integrating multiple scan engines**

Do the following when multiple scan engines are used to support the X9000 storage device:

- Configure the settings on each Symantec Scan Engine to be identical.
- Schedule LiveUpdate and Rapid Release to occur at the same time on all of the scan engines. This ensures that virus definitions are consistent.
Configuring Symantec AntiVirus™ for HP IBRIX X9000 Storage System

Recommendations while integrating multiple scan engines