Configuring Symantec™ Protection Engine for Network Attached Storage 7.0 for EMC Isilon OneFS
Configuring Symantec™ Protection Engine for Network Attached Storage 7.0 for EMC Isilon OneFS

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: 7.0

Legal Notice

Copyright © 2013 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
Configuring Symantec™ Protection Engine for Network Attached Storage 7.0 for EMC Isilon OneFS

This document includes the following topics:

- About software components
- How Symantec Protection Engine works with EMC Isilon OneFS
- About preparing for installation
- About configuring Symantec Protection Engine
- About configuring the EMC Isilon OneFS
- Recommendations while integrating multiple protection engines

About software components

Symantec Protection Engine for Network Attached Storage 7.0 provides virus scanning and repair capabilities for EMC Isilon OneFS.

Symantec Protection Engine for Network Attached Storage 7.0 is hereafter referred to as Symantec Protection Engine.

Configure the following components to add antivirus scanning to EMC Isilon OneFS:

- Symantec Protection Engine provides the virus scanning and repair services.
For more information, see the Symantec™ Protection Engine for Network Attached Storage 7.0 Implementation Guide.

- **EMC Isilon OneFS version 7.0**
  Some options are configured directly on the NAS server. No additional code is necessary to connect Symantec Protection Engine to the NAS server.

- **EMC Isilon OneFS version 6.5**
  Some options are configured directly on the NAS server. No additional code is necessary to connect Symantec Protection Engine to the NAS server.

## How Symantec Protection Engine works with EMC Isilon OneFS

Symantec Protection Engine provides virus scanning and repair capabilities for the EMC Isilon series of network-attached storage devices that support OneFS versions 6.5 and 7.0. Virus scanning and repair is provided for files on the Common Internet File System (CIFS).

The Internet Content Adaptation Protocol (ICAP) is used to communicate with Symantec Protection Engine. In a typical EMC Isilon NAS environment, a minimum of two protection engines are required to handle the scan volume. A maximum of four protection engines can be supported per EMC Isilon storage device. The Symantec Protection Engine service handles load balancing across multiple protection engines automatically.

### How are files scanned

The EMC Isilon storage device is configured to scan a file in real-time (that is, when a file is opened and when it is closed, if it has been modified). When a user tries to access a file from storage, a connection is opened with Symantec Protection Engine. The file is passed to the protection engine for scanning. After scanning is complete, the connection with the protection engine is closed.

Symantec Protection Engine indicates the scanning results to the EMC Isilon storage device after a file is scanned. The protection engine also returns the repaired file if the file is infected and can be repaired.

After the EMC Isilon storage device receives the scanning results, the file is handled in the following way: Only clean files are passed to the requesting user. 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. If the file is infected and cannot be repaired, the user is denied access to the file, and the infected file is quarantined. The user can also configure Symantec Protection Engine to quarantine an unrepairable file.
How caching works

Symantec Protection Engine 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 when the virus definitions on Symantec Protection Engine are updated and when the EMC Isilon storage device is restarted. Individual cache entries are updated whenever 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 EMC Isilon storage device and Symantec Protection Engine.

About specifying file types on EMC Isilon OneFS

Based on file extensions, Symantec Protection Engine determines, initially, whether a particular file should be passed for scanning. You can configure the types of files that are passed to Symantec Protection Engine for scanning when you set up the EMC Isilon storage device.

You can control the types of files that are scanned by using an exclusion or an inclusion list, or you can scan all files regardless of the extension. Configure the EMC Isilon storage device to pass all file types to the protection 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.

See “About configuring virus scanning on EMC Isilon OneFS” on page 20.

About specifying file types on Symantec Protection Engine

You can configure Symantec Protection Engine so that selected file types and file extensions are excluded from scanning. The setting on the protection engine is as important as the setting on the EMC Isilon storage device. This setting on the protection engine determines the types of files to scan upon receiving a file from the storage 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 the 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.

For more information, see the Symantec™ Protection Engine for Network Attached Storage Implementation Guide.

See “About specifying which file types to scan on the protection engine” on page 14.

About specifying the scan policy

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

- **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**: Scan files for viruses. Try to repair the infected file, and deny access to any irreparable file.
- **Scan and repair or delete**: Scan files for viruses. Try to repair the infected file, and delete any irreparable file.

About handling infected files on EMC Isilon OneFS

When an unrepairable infected file is found, the EMC Isilon storage device does not delete the file, even though the protection engine tells it to. Instead, the storage device quarantines the file and denies any access to the file. The quarantined files can be deleted or removed from quarantine by using the command-line interface on the EMC Isilon device.

For more information, see the appropriate EMC Isilon documentation.
About quarantining the unrepairable files on Symantec Protection Engine

You can configure Symantec Protection Engine to quarantine the files that are infected with viruses and are unrepairable. You must provide the host name or IP address of the Windows 2000 Server, Windows 2003 Server, or Windows 2008 Server computer that has the Symantec™ Quarantine Server installed.

For more information, see the **Symantec™ Protection Engine for Network Attached Storage Implementation Guide**.

About preparing for installation

The computer on which you plan to install Symantec Protection Engine must meet the system requirements that are listed in the **Symantec™ Protection Engine for Network Attached Storage Implementation Guide**.

After you have installed the Symantec Protection Engine, configure the virus scanning functionality on the EMC Isilon storage device.

About configuring Symantec Protection Engine

You must configure several settings on each Symantec Protection Engine that is used to support scanning for the EMC Isilon storage device.

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

The protection 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 the ICAP-specific options.

Configuring the ICAP-specific options

You can configure several settings that are specific to the ICAP protocol through the Symantec Protection Engine administrative interface. You can also change the protocol through the administrative interface if Symantec Protection Engine has already been configured to use another protocol. However, you must manually restart the Symantec Protection Engine service.
For more information about accessing the administrative interface, see the *Symantec™ Protection Engine for Network Attached Storage Implementation Guide*.

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

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bind address</td>
<td>Symantec Protection Engine detects all of the available IP addresses that are installed on the host. By default, Symantec Protection 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 Protection 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 Protection Engine binds to all of the scanning IP addresses that it detects. If Symantec Protection 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 Protection 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 Protection Engine.</td>
</tr>
<tr>
<td>Port number</td>
<td>The port number must be exclusive to Symantec Protection 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 Protection Engine can do any of the following:</td>
</tr>
<tr>
<td></td>
<td>■ Scan only: Scan files for viruses, but do nothing to infected files.</td>
</tr>
<tr>
<td></td>
<td>■ Scan and delete: 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></td>
<td>■ Scan and repair files: Scan files for viruses. Try to repair infected files, but do nothing to irreparable files (that is, do not delete the files from archive or container files).</td>
</tr>
<tr>
<td></td>
<td>■ Scan and repair or delete: Scan files for viruses. Try to repair infected files, and delete irreparable files from archive or container files.</td>
</tr>
</tbody>
</table>

To configure ICAP-specific options

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 ICAP.

   The configuration settings are displayed for the selected protocol.

   If you change the protocol setting from RPC to ICAP through the Symantec Protection Engine administrative interface, you must manually stop and restart the service.

4  Under ICAP Configuration, in the Bind address box, select the scanning IP addresses that you want to bind to Symantec Protection Engine. Select the Select All check box to select every IP address in the Bind address table.

   By default, Symantec Protection Engine binds to all interfaces.

5  In the Port number box, type the TCP/IP port number that the VSCAN service uses to pass files to Symantec Protection Engine for scanning.

   The default setting for ICAP is port 1344.
6 In the **Scan policy** list, select how you want Symantec Protection Engine to handle infected files.

The default setting is **Scan and repair or delete**.

7 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>

### About specifying which file types to scan on the protection engine

The settings on Symantec Protection Engine must be configured to specify the types of files to be scanned for viruses. The scan policy on the protection engine determines which files it should scan from the EMC Isilon storage 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 Protection Engine is configured by default to scan all files.

For more information, see the *Symantec™ Protection Engine for Network Attached Storage Implementation Guide*.

### Specifying which file types to scan

You can control which file types are scanned by specifying those extensions that you want to exclude from scanning, or you can scan all files regardless of extension.

**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**.

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:

- **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 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 Protection Engine for Network Attached Storage 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>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 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:

<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>

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 Protection Engine can be configured to impose limits on how container files are handled. This configuration reduces the exposure of the network 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 Protection Engine blocks container files based on their type, because only certain file types contain virus or malicious code. You can configure Symantec Protection 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™ Protection Engine for Network Attached Storage Implementation Guide.

Scheduling LiveUpdate to update virus definitions automatically

Scheduling LiveUpdate to occur automatically at a specified time interval ensures that Symantec Protection Engine always has the most current virus definitions. Schedule LiveUpdate to occur at the same time for each protection engine if you use multiple protection engines to support virus scanning. This scheduling ensures that all the 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 EMC Isilon storage device.

You must schedule LiveUpdate on each Symantec Protection Engine. After 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.

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**, check **Enable scheduled LiveUpdate**.

This option is enabled by default.

4 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 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 also 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 the 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 the Rapid Release definitions.
   
   This option is disabled by default.

4. In the Rapid Release interval box, specify the interval between which you want Symantec Protection Engine to download the Rapid Release definitions.
   
   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 configuring the EMC Isilon OneFS**

You must register at least one Symantec Protection Engine for each EMC Isilon storage device for which you want to provide virus scanning. You also must configure the virus scan functionality in accordance with the EMC Isilon documentation.

For more information, see the appropriate EMC Isilon documentation.

**About registering Symantec Protection Engine**

You must register at least one Symantec Protection Engine to provide the virus scanning for each EMC Isilon storage device. In a typical environment, a minimum
of two protection engines are required to handle the scan volume. Having one protection engine can cause denial-of-file access, in which case the engine does not respond. The EMC Isilon storage cluster handles load balancing across multiple protection engines automatically.

**Note:** You do not need to register the same protection engine with each EMC Isilon storage device. You can register different protection engines to different EMC Isilon storage devices. However, all of the protection engines that are registered with an EMC Isilon storage device must have identical configurations.

### About configuring virus scanning on EMC Isilon OneFS

You must configure virus scanning for each EMC Isilon storage device. You must configure the virus scan functionality through the Anti-Virus Settings page for each EMC Isilon storage device.

**Note:** The virus scan functionality for each EMC Isilon storage device accessing a protection engine must be configured identically to avoid inconsistency. The scan results and repair results for the infected files will be inconsistent if the settings differ for each device.

### Cluster antivirus scanning service

The antivirus scanning service of a cluster controls the scanning performed on a cluster.

After the scanning service is enabled, antivirus scans can be run automatically or manually. When the scanning service is disabled, all current scanning is halted and pending scans cannot proceed.

Before you can enable the antivirus scanning service, at least one ICAP protection engine must be configured for the cluster.

You can disable the antivirus scanning service of the cluster during system maintenance or to improve cluster performance. However, if threat detection and data security are priorities, keep the service enabled.

After you add an ICAP protection engine to a cluster, the engine is automatically enabled, provided that the engine is communicating with the cluster, as indicated by the green icon in the **Status** column. If the ICAP protection engine is not available or responding, the status indicator icon is red.
AntiVirus Global settings

Global settings enable you to specify how all antivirus scans are performed on the cluster. Some global settings can be overridden by individual scanning policies.

One particularly important antivirus global setting governs the response of the cluster when infected files are detected. The ICAP protection engines may be able to repair infected files. If repair is not possible, infected files can be quarantined to prevent end-user access, or truncated to render the threats harmless.

Other global settings enable you to restrict antivirus scanning to files of up to a specified maximum size, or restrict scans to only files with specific file extensions or specific file names. These settings can be overridden by individual antivirus scanning policies.

On-access scans govern whether files are scanned for viruses at the time that end users open or close them.

Table 1-2 describes the AntiVirus configuration in the EMC Isilon storage device.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action on Detection</td>
<td>Specifies which action the cluster and ICAP protection engine server will take if a virus is detected in files:</td>
</tr>
<tr>
<td>■ Alert only:</td>
<td>Generates an alert at the Warning level when a virus is detected, but does not quarantine or truncate the infected files.</td>
</tr>
<tr>
<td>■ Repair or quarantine:</td>
<td>Attempts to repair infected files by sending them to the Symantec Protection Engine servers. If repair is not possible, the infected files are quarantined on the cluster so that users cannot access them.</td>
</tr>
<tr>
<td>■ Repair or truncate:</td>
<td>Attempts to repair infected files by sending them to the Symantec Protection Engine servers. If repair is not possible, the infected files are truncated on the cluster to render them harmless.</td>
</tr>
<tr>
<td>■ Repair only:</td>
<td>Attempts to repair infected files by sending them to the Symantec Protection Engine servers. If repair is not possible, the cluster generates an alert at the Warning level.</td>
</tr>
<tr>
<td>■ Quarantine:</td>
<td>Prevents the users from opening or editing infected files. Storage administrators can remove infected files from quarantine using the File System Explorer of the cluster.</td>
</tr>
<tr>
<td>■ Truncate:</td>
<td>Reduces infected files to zero bytes in size to render them harmless. Truncating files cannot be reversed.</td>
</tr>
<tr>
<td>File Size Restriction</td>
<td>Specifies whether file size is used to determine which files are included in the antivirus scans:</td>
</tr>
<tr>
<td>■ Scan all files regardless of size:</td>
<td>Includes all files in antivirus scans regardless of how large they are.</td>
</tr>
<tr>
<td>■ Only scan files smaller than the maximum file size:</td>
<td>Excludes the files beyond a maximum size that is specified in bytes, megabytes, gigabytes, petabytes, or terabytes. The default setting is to scan files smaller than 2 GB in size.</td>
</tr>
</tbody>
</table>
Table 1-2  AntiVirus settings in EMC Isilon storage device (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filename Restrictions</td>
<td>Specifies whether to include or exclude files from antivirus scans based on their file names or extensions:</td>
</tr>
<tr>
<td></td>
<td>- Scan all files: By default, all files are scanned regardless of their names or extensions.</td>
</tr>
<tr>
<td></td>
<td>- Only scan files with the following extensions or file names: Restricts scanning to only those files matching file name or extension criteria.</td>
</tr>
<tr>
<td></td>
<td>- Scan all files except those with the following extensions or file names: Excludes scanning of files matching file name or extension criteria.</td>
</tr>
<tr>
<td>File Extensions</td>
<td>When Filename restrictions are enabled, this list identifies which file extensions are either included or excluded from antivirus scans. Click Edit list to add or modify file extensions, and optionally select from over 140 commonly used file extensions.</td>
</tr>
<tr>
<td>File names</td>
<td>When Filename restrictions are enabled, this list identifies which files are either included or excluded from antivirus scans. Click Edit list to add to or modify the list of files.</td>
</tr>
</tbody>
</table>

AntiVirus Scanning Policies

Antivirus scanning can be organized into the policies that specify which files on the cluster will be scanned and when.

Policies can be configured to:

- Scan files in specific root directories on the cluster.
- Run scans at scheduled times on a daily, weekly, monthly, or yearly basis.
- Run scans manually at any time by storage administrators.
- Enforce or ignore the global antivirus settings that restrict scans to certain file names, extensions, and maximum file sizes.

AntiVirus threat response

When infected files are detected on the cluster, you can configure the antivirus service to respond to the threats in several different ways. Some infected files can be repaired by the protection engine servers. If infected files cannot be repaired, they can be quarantined to prevent end users from accessing them.
Infected files can also be truncated, which reduces the files to zero bytes in size and renders the threat harmless.

**AntiVirus scan reports**

You can view antivirus reports that contain summary and detailed information about antivirus scans run on the cluster.

You can also export antivirus scan reports as comma-separated values (.csv) files. Any virus threats that are detected on the cluster are also reported as alerts, as are problems with the availability of third-party protection engine servers.

You can configure global antivirus settings to specify how long to retain antivirus scanning reports on the cluster before they are automatically purged.

**Recommendations while integrating multiple protection engines**

Do the following when multiple protection engines are used to support the EMC Isilon storage device:

- Configure the settings on each Symantec Protection Engine to be identical.
- Schedule LiveUpdate and Rapid Release to occur at the same time on all of the protection engines. This ensures that virus definitions are consistent.
- Configure the virus scan functionality to be identical for each EMC Isilon storage device in a group to avoid inconsistency. The scan results and repair results for infected files will be inconsistent if the settings differ for each device in a group.