Configuring Symantec™ Protection Engine for Network Attached Storage 7.8 for Hitachi Unified and NAS Platforms
Configuring Symantec™ Protection Engine for Network Attached Storage 7.8 for Hitachi Unified and NAS Platforms

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: 7.8

Legal Notice

Copyright © 2017 Symantec Corporation. All rights reserved.

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

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

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

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR
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:

http://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:

http://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 7.8 for Hitachi Unified and NAS Platforms

This chapter includes the following topics:

- About software components
- How Symantec Protection Engine works with the Hitachi Unified and NAS Platforms
- About preparing for installation
- About configuring Symantec Protection Engine
- About configuring the Hitachi NAS device
- Recommendations while integrating multiple protection engines

About software components

Symantec™ Protection Engine for Network Attached Storage provides virus scanning and repair capabilities for the Hitachi Unified and NAS Platforms.

Configure the following components to add antivirus scanning to the Hitachi NAS devices:

- Symantec™ Protection Engine for Network Attached Storage version 7.8 provides the virus scanning and repair services. For more information, see the Symantec™ Protection Engine for Network Attached Storage Implementation Guide.

- Hitachi Unified and NAS Platforms operating on HNAS OS version 12.0 or later. Some options are configured directly on the NAS device. No additional code is necessary to connect Symantec™ Protection Engine for Network Attached Storage to the device.
  - Hitachi NAS 3080
How Symantec Protection Engine works with the Hitachi Unified and NAS Platforms

Symantec Protection Engine provides virus scanning and repair capabilities for the Hitachi Unified and NAS Platforms that support HNAS OS version 12.0 or later. Virus scanning and repair are provided for files on the Common Internet File System (CIFS).

Internet Content Adaptation Protocol (ICAP) is used to communicate with Symantec Protection Engine. In a typical NAS environment, a minimum of two protection engines are required to handle the scan volume. A maximum of 32 protection engines can be supported per NAS device. The NAS service handles load balancing across multiple protection engines automatically.

How are files scanned

The Hitachi NAS 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, the NAS device opens a connection with Symantec Protection Engine. The device then passes the file to the protection engine for scanning. After scanning is complete, the device closes the connection with the protection engine.

Symantec Protection Engine indicates the scanning result to the NAS device after a file is scanned. After the 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 allowed access to the file, denied access to the file, or the file is deleted. User can configure these options on the Hitachi NAS device. The infected file is deleted by default.

How caching works

The NAS device caches the 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 Hitachi NAS device is restarted. Individual cache entries are updated whenever a stored file is changed.

Note: Symantec™ Protection Engine for Network Attached Storage is hereafter referred to as Symantec Protection Engine.
About specifying which file types are scanned

To specify the file types to be scanned for viruses, configure settings on both, the Hitachi NAS device and Symantec Protection Engine.

About specifying file types on the NAS device

Based on file extensions, the NAS device determines, initially, whether it should pass a file to Symantec Protection Engine for scanning. You can configure which files are passed to Symantec Protection Engine for scanning when you set up the Hitachi NAS device.

You can control which files are scanned by using an exclusion or an inclusion list, or you can scan all files regardless of extension. Configure the Hitachi NAS 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.

The virusscan command is used to configure the exclusion list.

**virusscan-exclusion-list-add <file-types>**

**Description**

The virusscan-exclusion-list-add command adds one or more file type extensions to the list of those which are to be excluded from virus scanning.

Options:

* <file types>*

A comma-separated list of file type extensions.

A wildcard '?' can be used to mean any single character. The matching is done per-character so the extension must match the length of the wildcarded extension. The wildcarded string "XL?" in the list will match ".XLS" and ".XLX" file extensions but will not match ".XLSX". To match ".XLSX" and ".XLS" files would require both to be added to the list (either with or without the wildcards - "XLS, XLSX", "XL?,XLS?" or "XL?,XL??").

Multiple wildcards are permitted within an extension. For example, "A?C?" will match any four letter extension with "A" as its first character and "C" as its third (AACA, ..., ABCD, ..., AZCZ).

There must be no whitespace between consecutive types.

**Examples**

To add the .bat, .com, .doc, .exe and .ppt types:

`virusscan-exclusion-list-add BAT,COM,DOC,EXE,PPT`
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 Symantec Protection Engine is as important as the settings on the NAS device. The setting on the protection 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.

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"

About specifying the scan policy

You configure the scan policy through the Symantec Protection command line 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 the NAS device

HNAS passes the clean files to the requesting user after it receives the scanning results. The stored version of the infected file is then replaced with the repaired file. The user is denied access to the file found to be infected and cannot be repaired. The infected file is subsequently deleted from HNAS. If a file has not been verified by a virus scan engine as clean, it will need to be scanned before it can be accessed.

Note: In case of infected read-only files, SPE can scan the files, but cannot repair or delete them. However, the file’s read only setting can be modified by using the HonorReadOnly command in order to repair or delete infected read only files.

If the file is infected, you are allowed access to the file, denied access to the file, or the file is deleted. You can configure these options on the NAS device. The infected file is deleted by default.

You can configure the NAS device to receive notifications when an infection is detected.
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 Symantec Protection Engine, configure the virus scanning functionality on the Hitachi Unified and NAS Platforms.

About configuring Symantec Protection Engine

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

---

**Note:** If you use multiple protection engines to support scanning, the configuration settings on each protection engine must be identical. LiveUpdate must schedule to occur at the same time on all protection engines so that 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 must configure the ICAP-specific options.

See "About configuring the Hitachi NAS device".

Configuring the ICAP-specific options

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

For more information about accessing the command line interface, see the *Symantec™ Protection Engine for Network Attached Storage Implementation Guide*.

*Protocol-specific options for ICAP* describes the protocol-specific options for ICAP.

### Table 2-1 Protocol-specific options for ICAP

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bind address</td>
<td>Symantec Protection Engine detects all 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.</td>
</tr>
</tbody>
</table>
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.

**Note:** 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.

<table>
<thead>
<tr>
<th>Port number</th>
<th>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.</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 the ICAP-specific options**

1. Go to the Symantec Protection Engine installation directory.
2. Set the ICAP protocol.

**Command:**

```
xmlmodifier -s //configuration/ProtocolSettings/Protocol/@value ICAP configuration.xml
```

**Allowed values:**

- **ICAP**

  Enables the ICAP protocol.
• RPC
  Enables the RPC protocol.

  **Default value:** ICAP

3. Specify the Bind address.

  **Command:**
  ```
  xmlmodifier -s //configuration/ProtocolSettings/ICAP/BindAddress/@value <value>
  configuration.xml
  ```

  **Allowed values:** Scanning IP addresses that you want to bind to Symantec.

  **Default value:** Symantec Protection Engine binds to all interfaces.

4. Specify the port number that the client application uses to pass files to Symantec.

  **Command:**
  ```
  xmlmodifier -s //configuration/ProtocolSettings/ICAP/Port/@value <value> configuration.xml
  ```

  **Allowed values:** Port number that is equal to or greater than 1024. No other program or service should use this port number. You must use the same port number for every scanning IP addresses that you want to bind to Symantec Protection Engine.

  **Default value:** 1344

5. Restart the Symantec Protection Engine service.

### Configuring the antivirus scan policy

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

#### To configure the antivirus scan policy

1. Go to the Symantec Protection Engine installation directory.
2. Enable the antivirus scanning.

  **Command:**
  ```
  xmlmodifier -s //policies/ThreatPolicies/AntiVirusScanning/@value <value> policy.xml
  ```

  **Allowed values:**

  - **true**
    Enables antivirus scanning.
  - **false**
    Disables antivirus scanning.

  **Default value:** true

3. Configure Symantec Protection Engine to do one of the following when an infected file is found.

  **Command:**
  ```
  xmlmodifier -s //policies/ThreatPolicies/Actions/AVActionPolicy/@value <value> policy.xml
  ```
Allowed values:
- 0 - Scan only
- 1 - Scan and repair
- 2 - Scan and repair or delete
- 3 - Scan and delete

Default value: 2 - Scan and repair or delete

Note: You must select Scan and repair or delete if you plan to quarantine the infected files that cannot be repaired.

4. Restart the Symantec Protection Engine service.

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 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 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 specify which files to scan

1. Go to the Symantec Protection Engine installation directory.
2. Enable extension policy to scan all files except those in the extension or type exclude lists.
   
   Command: `xmlmodifier -s //policies/ThreatPolicies/ExtensionPolicy/@value 2 policy.xml`

   Allowed values:
   - 0 - Disable
   - 2 - Exclude the files with below extension from AV scanning.

   Default value: 0

3. You can add or remove any file extension that you want to exclude from AV scanning at the below XPath in the `policy.xml` file.
   
   XPath: `//policies/ThreatPolicies/ExcludeList`

   Allowed values:
   You can add any file extension to the file extension exclude list (file extensions must begin with a period).

4. You can add or remove entries in the file type exclude list in the `policy.xml` at the below XPath:

   XPath: `//policies/ThreatPolicies/MIMEExcludeList`
Allowed values:

File types listed in: For more information about File types that you can add to the File type exclude list, see the Symantec™ Protection Engine for Network Attached Storage Implementation Guide.

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 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 scanprotectionengines to support virus scanning. This scheduling ensures that all protection engines have the same version of virus definitions. Having the same version of virus definitions is necessary for proper functioning of virus scanning on the Hitachi NAS device.

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

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

To schedule LiveUpdate to update virus definitions automatically

1. Go to the Symantec Protection Engine installation directory.
2. Enable LiveUpdate schedule.

Command:
xmlmodifier -s //liveupdate/Schedule/@enabled true liveupdate.xml

**Allowed values:**
- **true**
  Enables LiveUpdate.
- **false**
  Disables LiveUpdate.

**Default value:** true

3. In the LiveUpdate interval list, select the interval.

**Command:**

```
xmlmodifier -s //liveupdate/Schedule/Interval/@value <value>
```

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

**Default value:** 7200

4. Restart the Symantec Protection Engine service.

---

### Configuring Rapid Release updates to occur automatically

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

### Configuring Rapid Release updates to occur automatically

1. Go to the Symantec Protection Engine installation directory.
2. Configure Rapid Release updates to occur automatically.

**Command:**

```
xmlmodifier -s //liveupdate/RapidRelease/Schedule/@enabled true liveupdate.xml
```

**Allowed values:**
- **true**
  Enables Rapid Release updates.
- false
  Disables Rapid Release updates.
  **Default value:** false

3. In the Rapid Release interval specify the interval between which you want.

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

  **Allowed values:** You can select any number between 5 minutes and 120
  
  **Default value:** 30

4. Restart the Symantec Protection Engine service.

---

**About configuring the Hitachi NAS device**

You must register at least one Symantec Protection Engine for each Hitachi NAS device for which you provide virus scanning. You also must configure the virus scan functionality in accordance with the Hitachi documentation.

For more information, please see the *Hitachi NAS Platform Antivirus Administration Guide* that is included in the HNAS Platform Product Documentation Library disc.

See "**About configuring Symantec Protection Engine**"

**About registering Symantec Protection Engine**

You must register at least one Symantec Protection Engine to provide the virus scanning for each Hitachi NAS device. In a typical environment, a minimum of two protection engines are required to handle the scan volume per system. Having one protection engine can cause denial-of-file access, in which case the engine does not respond.

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

**About configuring virus scanning on the Hitachi NAS device**

You must configure virus scanning for each Hitachi NAS device. The virusscan command is used to manage virus scanning settings. It can be used to manage virus scan servers, view statistics, set the file types that are scanned and to request a full system scan.
**Note:** The virus scan functionality for each Hitachi NAS device accessing a protection engine must be configured identically to avoid inconsistency. The scan results and repair results for infected files will be inconsistent if the settings differ for each device.

```
```

**Options:**

- **-a, --all**
  Toggle functionality between scanning all files and scanning just those based on their extensions (see -I option for list of currently included file types).

- **-b, --enable <ip address>|host>**
  Enable a virus scan server that isn't currently in use. Host names can only be used for ICAP scanners.

- **-d, --deregister <ip address>|host>**
  Deregister a virus scan server that's currently registered. Host names can only be used for ICAP scanners. Note that in the case of RPC scanners, the virus scan server may simply re-register itself immediately. In this case, if you don't want the virus scan server to be used again, you should remove the current EVS's IP address(es) from the virus scan server's list of RPC clients.

- **-e, --delete <file types>**
  Delete the given file types from the list of file types to scan. Takes a comma-separated list.

- **-f, --default**
  Reset the list of file types to the default list.

- **-i, --include <file types>**
  Add the given file types to the list of file types to scan. Takes a comma-separated list. There can be a maximum of 250 entries in the list including the default types.

A wildcard '?' can be used to mean any single character. The matching is done per-character so the extension must match the length of the wildcarded extension. The wildcarded string "XL?" in the list will match .XLS and .XLX file extensions but will not match .XLSX extensions. To match .XLSX and .XLS files, for example, you would need to add both strings to the inclusion list (either with or without the wildcards - "XLS, XLSX", "XL?,XLS?" or ",XLS?,XL?").

Multiple wildcards are acceptable - for example "A?C?" would match any four letter extension with "A" as its first character and "C" as its third (AACCA, ..., ABCD, ..., AZCZ).

- **-l, --deleteall**
Delete all file types from the list of file types to scan.

- r, --reset
Reset the statistics.

- s, --fullscan
Request a full system scan - i.e. scan all files in the list of file types to scan, regardless of whether they've been scanned already. Files won't be scanned immediately, but when they're next opened.

- I, --list-inclusion
Display a list of file types to scan, useful when virus-scanning is disabled (when the virus-scanning is enabled the list is displayed anyway).

- B, --enable-best-effort-scanning
Enable "best-effort" scanning. With this mode enabled CIFS access to files is not denied if there are no valid servers available. If no scan-engine is available, access will be granted to the user to open the file with no scan being performed. If a scan-engine reports a non-virus-related error during a scan, access will also be granted (see NOTE). The file is not marked in the file-system as "clean" so future accesses will prompt another attempted scan.

**Note:** Access is also enabled for files that cause a scan-engine to refuse to scan. For example, scan-engines usually have a maximum depth of zip file they will scan into before giving up. In best-effort mode these files will be available to be read. The intention of this is that access will be allowed unless a scan-engine specifically marks a file as infected.

- N, --disable-best-effort-scanning
Disable "best-effort" scanning. The normal operating mode where CIFS access is denied if the system cannot perform a scan due to lack of scan-engines.

- v, --verbose-stats
Show verbose server statistics. Each server keeps track of a number of extra statistics which can be used to diagnose virusscan scan-engine problems.

### Recommendations while integrating multiple protection engines

Do the following when multiple protection engines are used to support the Hitachi NAS 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 Hitachi NAS 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 the group.