Configuring Symantec™ Protection Engine for HP 3PAR File Persona

*SPE Version 7.5.1*
## Contents

Abstract ........................................................................................................................................... 3  
About software components .................................................................................................................. 3  
About configuring Symantec Protection Engine .................................................................................. 4  
  Configuring the ICAP-specific options .............................................................................................. 4  
  About specifying which file types to scan on the protection engine ..................................................... 5  
  Specifying which file types to scan ...................................................................................................... 6  
  About specifying container handling limits .......................................................................................... 7  
  Scheduling LiveUpdate to update virus definitions automatically ....................................................... 7  
  Configuring Rapid Release updates to occur automatically ................................................................. 8  
About configuring antivirus services for HP 3PAR File Persona ............................................................ 9  
  Launching the SSMC .......................................................................................................................... 9  
  Configuration and management steps .................................................................................................... 9  
  Adding Symantec Protection Engine .................................................................................................... 10  
  Using the management console ........................................................................................................... 10  
  Using the command line interface ....................................................................................................... 10  
  Enabling or disabling antivirus on Virtual File Server ....................................................................... 10  
  Using the management console ........................................................................................................... 10  
  Using command line interface ............................................................................................................ 11  
  Enabling antivirus scans ...................................................................................................................... 11  
  Using the management console ........................................................................................................... 11  
  Using command line interface ............................................................................................................ 11  
  Defining protocol-specific policies ....................................................................................................... 11  
  Using the management console ........................................................................................................... 12  
  Using the command line interface ....................................................................................................... 12  
  Updating antivirus definitions .............................................................................................................. 13  
  Using the management console ........................................................................................................... 13  
  Using the command line interface ....................................................................................................... 13  
  Using antivirus schedule scan (AVSS) .............................................................................................. 13  
  Using the management console ........................................................................................................... 13  
  Using the command line interface ....................................................................................................... 13  
  Viewing, pausing, resuming, or stopping antivirus scan tasks ............................................................ 14
Using the management console ................................................................. 14
Using the command line interface ......................................................... 14
Viewing antivirus statistics ....................................................................... 14
Using the management console ................................................................. 14
Using the command line interface ......................................................... 14
Removing Symantec Protection Engine from the configuration .................. 15
Using the management console ................................................................. 15
Using the command line interface ......................................................... 15
Recommendations while integrating multiple protection engines .................. 15
Abstract
This document explains how to configure HP 3PAR File Persona for antivirus scanning capabilities using Symantec Protection Engine. This document is meant for users who are using HP 3PAR StoreServ with HP 3PAR File Persona and Symantec Protection Engine version 7.5.1.

About software components
HP 3PAR File Persona’s antivirus feature must be configured to enable scanning from Symantec Protection Engine. For file sharing protocols FTP, SMB, HTTP, and NFS, when antivirus is enabled on a file system, scans are triggered when a file is first read. Subsequent reads to the file do not trigger a scan unless the file has been modified or the virus definitions have changed. For CIFS, you must specify the file operations that trigger a scan (open, close, or both).

The scans are forwarded to the virus scan engine, which blocks the operation until the scan is complete. After a successful scan, if the file is found to be infected, the system reports permission denied error message as the result of the file operation. If the file is clean, the file operation is allowed to go through.

You can define antivirus exclusions on directories in a file system to exclude files from being scanned. When you define an exclusion rule for a directory, all files/folders in that directory hierarchy are excluded from antivirus scans based on the rule.
About configuring Symantec Protection Engine

You must configure several settings on each Symantec Protection Engine that is used to support scanning for HP 3PAR File Persona.

**Note:** If you use multiple protection engines to support scanning, the configuration settings on each protection engine must be identical. LiveUpdate must be scheduled 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.

**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 Symantec Protection Engine.

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

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

<table>
<thead>
<tr>
<th><strong>Table 1:</strong> Protocol-specific options for ICAP</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Option</strong></td>
</tr>
</tbody>
</table>
| Bind address | 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.  
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. |
| Port number | 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. |
| Scan policy | When an infected file is found, Symantec 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 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: Scan files for viruses. Try to repair infected files, and delete irreparable files from archive or container files.

**To configure the 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 start 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. Check **Select All** 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 NAS 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:
   - Click **Save** to save your changes. You can continue to make changes in the administrative interface until you are ready to apply them.
   - Click **Apply** to apply your changes. Your changes are not implemented until you apply them.

**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 HP 3PAR File Persona. 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.
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 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:
   - Click Save to save your changes. You can continue to make changes in the administrative interface until you are ready to apply them.
   - Click Apply to apply 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:
   - Click **Save** to save your changes. You can continue to make changes in the administrative interface until you are ready to apply them.
   - Click **Apply** to apply your changes. Your changes are not implemented until you apply them.

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

**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 scan protection engines 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 HP 3PAR File Persona 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. 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:
   • Click Save to save your changes. You can continue to make changes in the administrative interface until you are ready to apply them.
   • Click Apply to apply your changes. Your changes are not implemented until you apply them.

Configuring Rapid Release updates to occur automatically
You can configure Symantec Protection Engine to obtain uncertified definition updates with Rapid Release. You can configure Symantec Protection Engine to retrieve Rapid Release definitions every 5 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. On the Symantec Protection Engine administrative interface, in the left pane, click **System**.

2. Under **Views**, click **Rapid Release Content**.

3. In the content area under **Rapid Release Content**, select the **Enable scheduled Rapid Release** check box to enable automatic downloads of Rapid Release definitions. This option is disabled by default.

4. In the Rapid Release interval box, to specify the interval between which you want Symantec Protection Engine to download Rapid Release definitions, do any of the following steps:
   - Type the interval.
   - Click the up arrow or down arrow to select the interval.

   You can select any number between 5 minutes and 120 minutes. The default value is 30 minutes.

5. On the toolbar, select one of the following:
   - Click **Save** to save your changes. You can continue to make changes in the administrative interface until you are ready to apply them.
   - Click **Apply** to apply your changes. Your changes are not implemented until you apply them.

---

**About configuring antivirus services for HP 3PAR File Persona**

Managing the antivirus services and settings for the HP 3PAR File Persona can be accomplished by using either the HP 3PAR Command Line Interface (CLI) or the HP 3PAR StoreServe Management Console (SSMC).

**Launching the SSMC**

To log into the main console, browse to the server on which HP 3PAR StoreServ Management Console software is installed specifying https://<IP address or FQDN>:8443. (This is the default port number. Another port may have been assigned during software installation.) On the login screen, supply the username and password, click **Login** and the **Dashboard** screen is displayed.

**Configuration and management steps**

Initiating and managing antivirus scans and policies for HP 3PAR File Persona, can be done at either the Virtual File Server (VFS) level or the File Store level. The commands and procedures which follow will specify to which component they apply.

To configure the antivirus feature on an HP 3PAR File Persona cluster, complete these steps:

1. Adding Symantec Protection Engine
2. Enabling or disabling antivirus on Virtual File Server
3. Enabling antivirus scans
4. Defining protocol-specific policies
5. Updating antivirus definitions
6. Using antivirus schedule scan (AVSS)
7. Viewing, pausing, resuming, or stopping antivirus scan tasks
8. Viewing antivirus statistics

---
Adding Symantec Protection Engine

Using the management console
To add, edit, or remove a virus service engine (VSE) using the SSMC, follow these steps:

1. On the SSMC main menu, select **File Persona > Persona Configuration**.
2. In the list pane, select the system name and then select **Configure file persona** from the **Actions** menu.
3. On the dialog that opens, select the **Advanced options** check box.
4. On the **Antivirus Settings** panel, select **Enabled** or **Disabled** for the **Antivirus service** as appropriate.
5. Also, on the **Antivirus Settings** panel, select **Antivirus Servers** then select **Add**. Provide the IP address and Port of the antivirus Server in the dialog box and choose **Add** to complete or choose **Add+** if adding multiple VSEs at once.

Using the command line interface
To add, edit or remove a virus service engine using the HP 3PAR CLI, execute the

```
setfsav vse +/- <IP_address>:<port> command where:
```

+/- adds (+) or removes (-) the specified VSE.

```
<IP address>:<port> specifies the IP address and port number of an external virus scan engine. The default port number for a VSE is 1344, because it uses the ICAP protocol.
```

**Note:** Adding the `<IP_address>:<port>` to an empty VSE list automatically starts the antivirus service.

To enable antivirus services using the HP 3PAR CLI, execute the `startfsav svc` command.

To disable antivirus services using the HP 3PAR CLI, execute the `stopfsav svc` command.

Use the command `setfsav vse - <IP_address>:<port>` to remove the VSE. When the last `<IP_address>:<port>` is removed from the list the antivirus service is stopped automatically.

Enabling or disabling antivirus on Virtual File Server

Using the management console
Verify that the antivirus service is enabled for File Persona.

1. On the SSMC main menu, select **File Persona > Persona Configuration**.
2. In the list pane, select the system name and then select **Configure file persona** from the **Actions** menu.
3. On the dialog that opens, select the **Advanced options** check box.
4. On the **Antivirus Settings** panel, enable the **Antivirus service** as appropriate.

To enable antivirus on the Virtual File Server using the SSMC, follow these steps:

1. On the SSMC main menu, select **File Persona > Virtual File Servers**.
2. In the list pane, select the Virtual File Server name and then select **Modify antivirus policy** from the **Actions** menu.
3. On the **Dynamic scanning** panel, select **Enabled**.
4. On the **Vendor Information** panel, select **SYMANTEC**.

To disable antivirus on the Virtual File Server using the SSMC, follow these steps:
1. On the SSMC main menu, select **File Persona > Virtual File Servers**.
2. In the list pane, select the Virtual File Server name and then select **Modify antivirus policy** from the **Actions** menu.
3. On the **Dynamic scanning** panel, select **Disabled**.

**Using command line interface**

To verify that the antivirus service is enabled for File Persona using the HP 3PAR CLI execute the `showfsav svc` command. Execute the `showfsav` command with no options to review the configured VSE information.

To enable scanning and set the vendor type on the Virtual File System using the HP 3PAR CLI execute the `setfsav pol -scan enable -vendor SYMANTEC <vfs>` command where `<vfs>` is the name of the Virtual File Server.

To disable scanning on the Virtual File System execute the `setfsav pol -scan disable -vendor SYMANTEC <vfs>` command where `<vfs>` is the name of the Virtual File Server.

**Enabling antivirus scans**

**Using the management console**

To use SSMC to initiate an antivirus scan from a Virtual Files Servers screen, select **File Persona > Virtual File Servers** from the main SSMC menu. In the list pane, select the name and system of the Virtual File Server and then select **Create antivirus scan** from the **Actions** menu. Follow the instructions under **Schedule** to request a **Schedule pattern**.

To use SSMC to initiate an antivirus scan from a File Stores screen, select **File Persona > File Stores** from the main SSMC menu. In the list pane, select the name and system of the File Store and then select **Create antivirus scan** from the **Actions** menu. Follow the instruction on the dialog that opens. You can optionally specify the **Path** which is the subdirectory on the File Store where the scan will be initiated. Follow the instructions under **Schedule** to request a **Schedule pattern**.

**Using command line interface**

To initiate a scan on a virtual file server (VFS) or File Store using the HP 3PAR CLI execute the command:

```
startfsav scan [-fpg <fpgname>] [-fstore <fstore> [-path <path_name>]] <vfs_name>
```

Where:

- `scan` starts or resumes a paused antivirus scan.
- `-fpg <fpg_name>` specifies the name of the File Provisioning Group in which the VFS was created.
- `-fstore <fstore>` specifies the File Store name.
- `-path <path_name>` specifies the path, on the containing File Store, on which the scan should be initiated.

**Defining protocol-specific policies**

Use the HP 3PAR OS CLI command `showfsav` to display current virus scan engines by IP addresses and port numbers.

To display the status of antivirus services using the SSMC, follow these steps:

1. On the main menu in the SSMC, select **File Persona > File Persona Configuration**.
2. Select the pull down menu Overview panel and choose Antivirus Settings.

Using the management console
To configure antivirus policies using the SSMC:

1. On the main SSMC menu, select File Persona > Virtual File Servers to enter the Virtual File Servers screen.
2. From the list panel select the name of the Virtual File Server then choose Antivirus from the Overview panel.
3. Select the Actions menu and then select Modify antivirus policy.
4. Follow the instructions on the dialog that opens.

Using the command line interface
To configure antivirus policies using the HP 3PAR CLI, execute the setfsav pol command with the following options:

- [-fileop {open|openclose|inherit}]
- [-unavail {allow|deny|inherit}]
- [-excludesize {<size>|inherit}]
- [-excludeext {<ext>[,<ext>...]|inherit}]
- [-inheritall] [-fpg <fpgname>] [-fstore <fstorename>] <vfsname>

Where:

- fstore <fstorename> specifies the File Store name.
- fpg <fpgname> specifies the name of the File Provisioning Group.
- inheritall inherits all the settings from the VFS for the specified File Store, overriding previous setting in File Store. This is only valid when –fstore option is used.
- fileop specifies the policy that determines which file operations trigger antivirus scans. The policies are:
  - open – scans on file open.
  - openclose – scans on file open and file close.
  - inherit – inherits the fileop settings from VFS.

If a policy is not specified, the default is open when applied to a VFS and inherit when applied to a File Store.

- unavail specifies the scan policy to determine how targeted file operation are handled when an external VSE is not available. The policies are:
  - allow – allows all operations triggering scans to run to completion.
  - deny – blocks all operations triggering scans and returns with an error.
  - inherit – inherits the unavail settings from VFS.

If a policy is not specified, the default is allow when applied to a VFS and inherit when applied to a File Store.
-excludesize excludes all files larger than the specified size (MB). The value of size is an integer from 0 to 2147483647.

If this option is not specified or size is 0, all files will be included in the antivirus scan. If inherit is specified, the excludesize setting will be inherited from VFS.

-excludeext excludes all files having the specified extension. If this option is not specified or ext is ", all files will be included in the antivirus scan. If inherit is specified, the excludeext will be inherited from VFS.

<vfsname> specifies the Virtual File Server name.

Updating antivirus definitions
If the virus definitions on the VSE are not in sync with the virus definitions on the HP 3PAR StoreServ Storage system, files already scanned may not have been scanned based on the updated virus definitions. When a new file is read on the HP 3PAR StoreServ Storage system, the virus definitions are automatically updated with the definitions from the VSE.

Using the management console
To update virus definition using the SSMC, follow these steps:

1. On the main SSMC menu, select File Persona > File Persona Configuration.
2. From the Overview panel, select Antivirus Settings.
3. Select the Actions menu and then select Update virus definition.
4. Follow the instruction on the dialog that opens.

Using the command line interface
Execute the startfsav update command to update virus definitions using the HP 3PAR CLI.

Using antivirus schedule scan (AVSS)

Using the management console
To schedule an antivirus scan for a VFS using the SSMC, follow these steps:

2. In the list pane, select Virtual File Server name and then select Create antivirus scan from the Actions menu.
3. In the Schedule panel, select Schedule pattern.
4. Follow the instructions which apply to your schedule pattern selection.

To schedule an antivirus scan for a File Store using the SSMC, follow these steps:

1. On the SSMC main menu, select File Persona > File Stores.
2. In the list pane, select File Store name and then select Create antivirus scan from the Actions menu.
3. In the Schedule panel, select Schedule pattern.
4. Follow the instructions which apply to your schedule pattern selection.

Using the command line interface
To schedule antivirus commands using the HP 3PAR CLI use the createsched command.
Viewing, pausing, resuming, or stopping antivirus scan tasks

Using the management console
To manage antivirus scans for a VFS using the SSMC, follow these steps:
2. In the list pane, select Virtual File Server name and then select Managing existing antivirus scans from the Actions menu.
3. Highlight the task you wish to manage and then choose Stop, Pause or Resume as appropriate.

To manage antivirus scans for a File Store using the SSMC, follow these steps:
1. On the SSMC main menu, select File Persona > File Stores.
2. In the list pane, select the File Store name and then select Managing existing antivirus scans from the Actions menu.
3. Highlight the task you wish to manage and then choose Stop, Pause or Resume as appropriate.

Using the command line interface
To stop or pause a scan on a Virtual File Server (VFS) or File Store using the HP 3PAR CLI:
1. Execute the stopfsav scan [-pause] [-fpg fpgname] [-fstore fstore] <vfs> <scan_id> command, where -pause pauses, rather than stops, the specified scan.
2. To resume a paused scan, using the HP 3PAR CLI, execute the startfsav scan [-resume <scan_id>] [-fpg <fpgname>] [-fstore <fstore>] <vfs> command where the specified <scan_id> corresponds to an ongoing scan in the paused state.

Viewing antivirus statistics

Using the management console
To manage quarantined files using the SSMC, follow these steps:
1. On the main SSMC menu, select File Persona > File Stores.
2. From the list panel select a File Store then select Manage Antivirus Quarantine from the Actions menu.
3. Select Export, Move, Delete, or Reset as appropriate.

If the Delete action is chosen, the Delete Quarantined Files dialog opens. If you are not sure if these quarantined files should be deleted, click Cancel; otherwise, click Delete to start the action and close the dialog.

Using the command line interface
To manage the quarantined files from the HP 3PAR CLI execute the command:

```
setfsav quar {exportlist|move|reset|delete|clearcount} [-fpg <fpgname>] [-fstor <fstore>] <vfs>
```

Only 3,000 quarantined files can be exported at a time. The list of 3,000 quarantined files is located at /<fpg>/<vfs>/admin/AV/Quarantine/quar_ifs1_AV.txt. You must reset, move, or delete the set of 3,000 files from any previous exports before exporting another set of files.

To delete quarantined files on the StoreServ using the HP 3PAR CLI, execute the command:

```
setfsav quar delete [-fpg <fpg_name>] [-fstore <fstore>] <vfs>
```

Where:
quar specifies the management of quarantined files.
delete specifies the quarantined files under specified in the specified VFS and File Store are deleted.

<fpg_name> specifies the name of the FPG to which the VFS belongs.

<fstore> specifies the name of the File Store.

<vfs> specifies the name of the Virtual File Server.

**Removing Symantec Protection Engine from the configuration**

**Using the management console**
To remove a virus service engine (VSE) using the SSMC, follow these steps:

1. On the SSMC main menu, select **File Persona > Persona Configuration**.
2. In the list pane, select the system name and then select **Configure file persona** from the **Actions** menu.
3. On the dialog that opens, select the **Advanced options** check box.
4. On the **Antivirus Settings** panel, select **Disabled** for the **Antivirus service** as appropriate.
5. Also, on the **Antivirus Settings** panel, select **Antivirus Servers** then select X that appears next to each VSE IP Address and Port entry.

**Using the command line interface**
To remove a virus service engine using the HP 3PAR CLI, execute the command:

```
setfsav vse - <IP_address>:<port>
```

Where:

- removes the specified VSE.

<IP address>:<port> specifies the IP address and port number of an external virus scan engine. The default port number for a VSE is 1344, since it uses ICAP protocol.

When the last <IP_address>:<port> is removed from the list the antivirus service is stopped automatically.

**Note:** Use caution when using the `setfsav vse` command without any options as this will clear out the list of VSEs.

**Recommendations while integrating multiple protection engines**
It is recommended to add at least one additional VSE to increase VSE availability and improve the performance for virus scanning tasks. When multiple VSEs are added to the cluster, all incoming scan requests are distributed in a round-robin fashion.

Locate the VSEs physically close to the StoreServ systems to reduce network latency and maintain optimum file access time.