Configuring Symantec Protection Engine™ for Network Attached Storage

Dell® FluidFS® 4.0
## Contents

Abstract ........................................................................................................................................... 3  
About software components ................................................................................................................. 3  
How does FluidFS antivirus protect data on FluidFS cluster ............................................................ 3  
Preparing for installation ..................................................................................................................... 4  
Configuring Symantec Protection Engine .......................................................................................... 4  
  Configuring the ICAP-specific options .............................................................................................. 4  
About specifying which file types to scan on the protection engine .................................................. 6  
Specifying which file types to scan ...................................................................................................... 6  
About specifying container handling limits ......................................................................................... 8  
Scheduling LiveUpdate to update virus definitions automatically ..................................................... 8  
Configuring Rapid Release updates to occur automatically .............................................................. 9  
NAS antivirus server specifications ...................................................................................................... 10  
Configuring antivirus scanning for FS7600 with FluidFS v4 .......................................................... 10  
  Adding a NAS antivirus server ......................................................................................................... 10  
    Prerequisites .................................................................................................................................. 11  
    Steps ............................................................................................................................................. 11  
  Modifying a NAS antivirus server ...................................................................................................... 11  
    Steps ............................................................................................................................................. 11  
  Deleting a NAS antivirus server ........................................................................................................ 11  
About status of NAS antivirus servers ............................................................................................... 12  
About NAS antivirus clusterwide defaults ......................................................................................... 12  
  Enabling the NAS antivirus service for a cluster ............................................................................. 12  
  Excluding file types and directory paths from scans on a cluster .................................................... 13  
  Enabling the NAS antivirus service on a SMB share ....................................................................... 13  
  Excluding file types on a SMB share ................................................................................................. 14  
  Monitor the NAS antivirus service .................................................................................................. 14  
NAS directory path and file type scan exclusions .............................................................................. 14  
  Modifying a directory path for a cluster ......................................................................................... 15  
  Excluding directory paths for a SMB share ...................................................................................... 16  
  Modifying file-type filtering clusterwide .......................................................................................... 16
Modifying file-type filtering for a SMB share ................................................................. 16
Antivirus policy .................................................................................................................. 17
Access infected files ......................................................................................................... 17
Configuring antivirus scanning for FS8600 with FluidFS v4 ............................................ 18
Configuring antivirus scanning .......................................................................................... 18
Adding a NAS antivirus server .......................................................................................... 18
Deleting an antivirus server ............................................................................................... 19
Enabling antivirus scanning for a SMB share ................................................................. 19
Allowing or denying access to files larger than the antivirus scanning file size threshold for a
SMB share ......................................................................................................................... 20
Changing the antivirus scanning file size threshold for a SMB share ................................. 20
Including or excluding file extensions and directories in antivirus scanning for a SMB share .. 21
Disabling antivirus scanning for a SMB share .................................................................. 22
Viewing antivirus events ................................................................................................. 22
Appendix ............................................................................................................................ 22
Excluding files and directory paths from scans ................................................................. 22
Supported antivirus applications ...................................................................................... 22
Abstract
This document explains how to configure Dell FluidFS NAS for antivirus scanning capabilities using Symantec Protection Engine. This document is meant for users who are using Dell FluidFS version 4.0 with Symantec Protection Engine version 7.5.1.

About software component
Symantec™ Protection Engine for Network Attached Storage provides virus scanning and repair capabilities for Dell FluidFS devices.

Configure the following components to add antivirus scanning to Dell FluidFS devices:

- Symantec™ Protection Engine for Network Attached Storage version 7.5.1
  Provides the virus scanning and repair services. Refer the Symantec Protection Engine for Network Attached Storage Implementation Guide for information on system requirements, installation, and configuration.

- Dell FluidFS version 4.0. The devices are:
  - FS7600
  - FS8600

How does FluidFS antivirus protect data on FluidFS cluster
The FluidFS cluster antivirus service provides real-time antivirus scanning of files stored in SMB shares. The antivirus service applies only to SMB shares; NFS is not supported. The scan operation is transparent to the client, subject to the availability of an antivirus server.

A file is scanned only when a client tries to open the file (not when an infected file is written, a file is opened to read/modify attributes, old files are opened for re-write, and so on).

The anti-virus service consists of two components:

- One or more network-accessible computers running Symantec Protection Engine, a third-party, ICAP-enabled antivirus application that provides the antivirus scanning service to the FluidFS cluster.

- A FluidFS cluster anti-virus scanning policy that specifies file extensions and directories to exclude from scans, an antivirus scanning file size threshold, and whether to allow or deny files larger than the file size threshold.

When a SMB share client requests a file from the FluidFS cluster, the FluidFS cluster passes the file to Symantec Protection Engine for scanning and then takes one of the following actions:

- If the file is virus-free, the FluidFS cluster permits client access. The FluidFS cluster does not scan that file again, providing it remains unmodified since the last check.

- If the file is infected, the FluidFS cluster denies client access. There is no indication to the client that the file is infected. The client experience is:
- A file deletion returns a system-specific "file not found" state for a missing file, depending on the client’s computer.

- An access denial might be interpreted as a file permissions problem.

Only storage administrators can recover an uninfected version of the file, or access and process the infected file. To gain access to an infected file, you must connect to the SMB share through another SMB share on which the antivirus service is disabled. Otherwise, the FluidFS cluster recognizes the file as infected, and denies access. You may also access the file through an NFS export, because NFS does not support antivirus.

File transfers between the FluidFS cluster and the antivirus server are not encrypted. Therefore, Dell recommends protecting/restricting the communication.

**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 FluidFS.

**Configuring Symantec Protection Engine**

You must configure several settings on each Symantec Protection Engine that is used to support scanning for FluidFS.

*Note*: If you use multiple protection engines to support scanning, the configuration settings on each protection engine must be identical. LiveUpdate must 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>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. 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>
<tr>
<td>Scan policy</td>
<td>When an infected file is found, Symantec Protection Engine can do any of the following:</td>
</tr>
</tbody>
</table>

- Scan only: Scan files for viruses, but do nothing to infected files.                                                                                                                                   |
- Scan and delete: Scan files for viruses, and delete any infected files that are embedded in archive or container files without trying to repair.                                                              |
- Scan and repair files: 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 FluidFS. 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:
   - 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 FluidFS 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 the virus scan functionality on FluidFS 4.0**

After you have installed and configured Symantec Protection Engine, configure the virus scanning functionality on FluidFS. The procedure varies amongst the different devices (FS7600 and FS8600)

**NAS antivirus server specifications**

The following requirements apply for antivirus servers:

- You must have a system (Cluster) with FluidFS V4 or later installed.  
  **Note:** Make sure that you are not using any earlier version of FluidFS.

- The server hosting Symantec Protection Engine must be accessible by the network. Dell recommends that the server be located on the same subnet as the NAS cluster.

- The server must run certified ICAP-enabled antivirus software such as Symantec Protection Engine.

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

**Configuring antivirus scanning for FS7600 with FluidFS v4**

Before you configure antivirus scanning, you may want to understand *How does FluidFS antivirus protect* data.

See **Excluding files and directory paths from scans** and **Supported antivirus applications** for more information.

**Adding a NAS antivirus server**

Before you can add and enable the NAS antivirus service and configure scanning on NAS SMB shares, you must:

- Install Symantec Protection Engine on the external antivirus servers.

- Set up Symantec Protection Engine as a network-accessible service in accordance with the user instructions for the antivirus software. See **Configuring Symantec Protection Engine**.

When you have installed Symantec Protection Engine, you can then add up to four antivirus servers, making these servers available to the NAS cluster. If an antivirus server becomes unavailable, NAS antivirus posts an event to the Group. For more information about monitoring events and event notifications refer the *Dell*® *EqualLogic Group Manager*® *Administrator’s Manual*. 
**Prerequisites**

To add NAS antivirus servers, you need the following information:

- The host name or IP address of up to four network-reaching servers on which you have previously installed Symantec Protection Engine. Use the Group Manager CLI to ping the server’s IP address for verification. If a server is unreachable, you cannot add it.

- A port number for the service, or you can use the default port number of 1334.

  **Note:** You need an alternate port number only if you intend to run multiple instances of the antivirus software on the same server (perhaps for use by other clients). However, Dell recommends a single instance per server, dedicated to the NAS antivirus service.

**Steps**

1. Click **Group**, expand **Group Configuration**, and select the NAS cluster.

2. Click the **Advanced** tab and go to the **Antivirus Servers** panel.

3. Click **Configure Antivirus Servers** and then click **Add**.

4. Enter the name or IP address of a computer providing the antivirus service.

5. Enter a port number or select **Use default port (1344)**.

6. Click **OK**.

You can now configure and enable NAS antivirus scanning, as NAS clusterwide defaults or on individual SMB shares.

**Modifying a NAS antivirus server**

You must add a minimum of one and maximum of four antivirus servers as described in Adding NAS Antivirus Servers. You can then modify antivirus servers as required.

**Steps**

1. Click **Group**, expand **Group Configuration**, and select the NAS cluster.

2. Click the **Advanced** tab.

3. Click **Configure Antivirus Servers** to go to the **Configure Antivirus Servers** panel.

4. Select one or more servers from the list and click **Modify**. The **Modify Antivirus Server** dialog box appears.

5. In the dialog box, change the server name or IP address.

6. In the **Port** field, enter the port number or click **Use default port**.

7. Click **OK** to confirm your changes.

**Deleting a NAS antivirus server**

You cannot delete the last server unless you first allow any in-progress operations to complete and you disable NAS antivirus on all SMB shares.
Note: Reducing the number of available antivirus servers might affect file access performance. To delete a NAS antivirus server:

1. Click Group, expand Group Configuration, and select the NAS cluster.
2. Click the Advanced tab.
3. Click Configure Antivirus Servers to go to the Configure Antivirus Servers panel.
4. Select one or more servers from the list and click Delete. When prompted, confirm the deletion.

About status of NAS antivirus servers
You cannot actively determine the status of Symantec Protection Engines from within Group Manager. Therefore, you cannot know whether antivirus servers are present and working. If no antivirus hosts are available, the following error message is logged to Group events:

No antivirus hosts are accessible. Virus scanning is not possible. SMB shares configured with antivirus scan will not be accessible.

NAS antivirus allocates scanning operations to the Symantec Protection Engines to maximize the available scanning bandwidth. The fewer the available antivirus servers, the more time required to scan files. If you have only one Symantec Protection Engine, you cannot delete that server until you first disable NAS antivirus on all SMB shares.

About NAS antivirus clusterwide defaults
NAS antivirus clusterwide defaults apply automatically to all newly created SMB shares. The defaults do not apply to any existing SMB shares for which you have manually configured share-specific NAS antivirus settings.

To enable NAS clusterwide antivirus defaults, follow the steps below. If you unconfigure the NAS antivirus service, you cannot modify the clusterwide defaults. However, if you subsequently reconfigure the service, the defaults that were previously in place are preserved. In addition, you must configure an antivirus server before you can specify clusterwide defaults.

1. Click Group, expand Group Configuration, and select the NAS cluster.
2. Click the Advanced tab and go to the Antivirus Defaults for SMB shares panel.
3. Check Enable virus scanning.
4. Click the Save icon at the top of the NAS cluster screen to save your changes.

Note: You cannot navigate away from the NAS cluster screen without confirming that you want to discard or save your changes.

When you have enabled antivirus defaults, you can configure the ability to control which file types or directories are scanned.

Enabling the NAS antivirus service for a cluster
You can enable the NAS antivirus service for the entire cluster. When you configure or modify the default NAS antivirus settings for a NAS cluster, the defaults apply to all newly created SMB shares.

1. Click Group, expand Group Configuration, and select the NAS cluster.
2. Click the Advanced tab and go to the Antivirus Defaults for SMB shares panel.

3. Check or uncheck Enable virus scanning.

4. Click the Save All Changes icon on the top task bar to save the current selections. After you enable the antivirus service, you can:
   - Exclude file extensions from the scan.
   - Exclude directory paths from the scan.

Excluding file types and directory paths from scans on a cluster

1. Prepare a list of file extensions for files that you want to exclude from scans:
   - Include variants of those extensions, such as docx and doc to specify Microsoft Word documents.
   - Use only numbers, letters, underscores, and the $ character in the extensions.

2. Click Group, expand Group Configuration, and select the NAS cluster.

3. Click the Advanced tab and go to the Antivirus Defaults for SMB shares panel.

4. In either the File Extensions to Exclude or Directory Paths to Exclude subpanel, click Add to open the Add List Item dialog box.

5. Enter a file extension such as xls or ppt. Do not enter the period (.) that separates a file extension from the file name.

6. Click OK to add the extension to the list of excluded files.

7. Repeat this process to add more file extensions.

8. Click the Save All Changes icon at the top of the screen.

Note: You also use this process to add directory paths for exclusion from antivirus scans. Make sure you click the Save All Changes icon at the top of the screen to complete the process.

Enabling the NAS antivirus service on a SMB share

You can enable the NAS antivirus service for individual SMB shares. To find out whether antivirus scanning is enabled for a particular SMB share, see Displaying SMB shares in a NAS Container.

Note: You cannot configure the antivirus service when you create a SMB share at the same time as you create a NAS Container. You must configure the antivirus service when you modify a SMB share.

1. Open the NAS view, then select the NAS container on which the SMB share resides.

2. Click the SMB SHARES shares tab to display a list of SMB shares.

3. Select a SMB share.

4. Click Modify SMB SHARES Share, then click the Antivirus Settings tab.

5. Check or uncheck Enable virus scanning.

6. Click OK.
In the list of SMB shares, the column titled Virus scanning now reads enabled for this share. After you enable the antivirus service, you can:

- Control which file extensions are excluded from being scanned.
- Control which directories are excluded from being scanned.

**Excluding file types on a SMB share**

1. Prepare a list of file extensions for files that you want to exclude from scans:
   - Include variants of those extensions, such as docx and doc to specify Microsoft Word documents.
   - Use only numbers, letters, underscores, and the $ character for the extensions.
2. Open the NAS view, then select a NAS container name.
3. Click the **Advanced** tab and go to the Antivirus Defaults for SMB shares panel.
4. Click the **SMB shares** tab to display a list of SMB shares in this NAS container.
5. In either the **File Extensions to Exclude or Directory Paths to Exclude** subpanel, click **Add** to open the **Add List Item** dialog box.
6. Enter a file extension such as xls or ppt. Do not enter the period (.) that separates a file extension from the file name.
7. Click **OK** to add the extension.
8. Repeat steps 4 to 6 to add more file extensions to exclude from the scan.
9. Click the **Save All Changes** icon at the top of the screen.

You can also configure the specifications for large file handling from the Antivirus Defaults for SMB shares panel:

1. In the Exclude files larger than field, enter the file-size limitation for the antivirus scan.
2. Select a unit (MB, GB, or TB) from the drop-down menu.
3. Click the **Save All Changes** icon at the top of the screen.

**Monitor the NAS antivirus service**

If you have configured NAS antivirus, you can monitor which SMB shares are using NAS antivirus.

1. Click **NAS**, expand a NAS cluster, expand **Local Containers**, and select a NAS container.
2. Click the **SMB SHARES** shares tab.
3. In the **Virus Scanning** column, determine which shares have virus scanning enabled and disabled.

**NAS directory path and file type scan exclusions**

You can control what directory paths and file types are scanned across a cluster or on SMB shares as follows:
- Directory paths to exclude—Specified as a path such as /tmp/logs (alternatively, folders and subfolders)
- File types to exclude—Specified by file extension (file type)

To exclude directory paths and file types from antivirus scans across clusters and on SMB shares:

- Specify directory paths to exclude
- Specify file types to exclude

You can specify file extension and path strings using the formats specified in the following table.

<table>
<thead>
<tr>
<th>Entity</th>
<th>Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>Directory path string</td>
<td>Forward slash (/) separated string of directories (folders), such as /user/programs/data/tmp</td>
</tr>
<tr>
<td>File extension string</td>
<td>Alphanumeric string such as docx or blend1</td>
</tr>
</tbody>
</table>

The following table describes permitted characteristics of file extensions and directory paths.

<table>
<thead>
<tr>
<th>Characteristic</th>
<th>File Extensions</th>
<th>Directory Paths</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default data</td>
<td>No default</td>
<td>No default</td>
</tr>
<tr>
<td>Default setting</td>
<td>Scan all files</td>
<td>Exclude no file extensions</td>
</tr>
<tr>
<td>Max characters</td>
<td>254 characters</td>
<td>254 ASCII characters per line item (path)</td>
</tr>
<tr>
<td>Wildcards</td>
<td>None</td>
<td>* (asterisk) and ? (question mark)</td>
</tr>
</tbody>
</table>

**Note:** Wildcards match only a single directory component, such as /user/*/tmp or /user/t?p.

**Modifying a directory path for a cluster**

You can specify the default NAS antivirus settings for a NAS cluster. These defaults apply to all newly created IFS shares, but the configuration of existing shares does not change. To modify a directory path for a cluster:

1. Click **Group**, expand **Group Configuration**, and select the NAS cluster.
2. Click the **Advanced** tab and go to the **Antivirus Defaults for SMB shares** panel.
3. Either:
   - Click **Add**, enter a directory path, and click **OK**.
   - Select a directory path, click **Modify**, edit the directory path as required, and click **OK**.
   - Select a directory path, click **Delete**, and click **Yes** to confirm the delete.
4. Click **OK**.
5. Click the **Save All Changes** icon at the top of the screen.
Excluding directory paths for a SMB share
You can exclude directory paths for a specific SMB share when you create a SMB share or when you subsequently modify the NAS antivirus settings for a SMB share.

1. Open the NAS view, then select a NAS container name.
2. Click the SMB shares tab.
3. Select a share and click Modify SMB Shares.
4. Click the General tab to determine the root of the mapped share.
5. Click the Antivirus Settings tab.
6. Click Add in Directory paths to exclude to open the Add List Item dialog box.
7. Enter a folder path based on the root of the mapped share.
   
   **Note:** In some cases, such as with .zip files and other archives, the antivirus server's settings override the NAS antivirus threat policies. Infected files are processed according to the antivirus server's configuration. Dell recommends coordinating the antivirus server's own policies with those of the NAS antivirus server to ensure that the system takes consistent action when it finds infected files.
8. Click OK.
9. Repeat the previous steps to add additional directory paths.
10. Click OK to close the Modify SMB share wizard.

Modifying file-type filtering clusterwide
When you configure or modify the default NAS antivirus settings for a NAS cluster, the defaults apply to all newly created SMB shares.

1. Click Group, expand Group Configuration, and select a NAS cluster.
2. Click the Advanced tab.
3. In the Antivirus Defaults for SMB Shares panel, either:
   - Click Add, enter a file extension to filter from antivirus scanning, and click OK.
   - In File extensions to exclude, select an extension, click Modify, change the extension, and click OK.
   - In File extensions to exclude, select an extension, click Delete, and click Yes to confirm.
4. Modify other file extensions as appropriate.
5. Click the Save All Changes icon at the top of the screen.

Modifying file-type filtering for a SMB share
You can modify the NAS antivirus settings for an individual SMB share.

1. Click NAS, expand NAS Containers, and select a NAS container.
2. Select the **SMB Share** tab.

3. In **SMB Shares**, right-click a SMB share and select **Modify SMB Share**.

4. In the **Modify SMB share** dialog box, click the **Antivirus Settings** tab.

5. In **File extensions to exclude**, either:
   - Click **Add**, enter a file extension to filter from antivirus scanning, and click **OK**.
   - In **File extensions to exclude**, select an extension, click **Modify**, change the extension, and click **OK**.
   - In **File extensions to exclude**, select an extension, click **Delete**, and click **Yes** to confirm.

6. Repeat to add, modify, or delete additional file extensions.

7. Click **OK**.

**Antivirus policy**

Depending on the antivirus policy, a file could be deleted immediately or made inaccessible to users and programs.

If the antivirus server or NAS cluster’s default setting causes file deletion, you can only recover a previous (uninfected) file. For example, you can recover a deleted file from a NAS container snapshot. The antivirus policies that result only in access denial are:

- **Quarantine file** (default)
  Quarantining a file involves the following steps:
  - The file is copied to a .quarantine folder at the volume root and is accessible only by administrators.
  - The file name is changed to include a string that specifies the date and identifies the file as infected.
  - File permissions are changed to permit access only by the root user.

- **Prevent file access**
  The file remains in place, but file permissions are changed to permit access only by an administrator.

**Access infected files**

Only administrators can access infected files. Infected files can be accessed through an NFS export. However, NAS antivirus does not support NFS exports.

**To access infected files:**

1. Log in to the group as an administrator.

2. Navigate to the NAS cluster and NAS container where the infected file is quarantined (or is in a denied access state).
3. Create a SMB share with a directory path to the directory that contains the infected file (such as the .quarantine directory).

   **Caution**: Do not enable NAS antivirus on this new SMB share.

4. Move the file to a location where you can either safely scan and disinfect the file according to the instructions provided by the antivirus software vendor, or otherwise dispose of the file.

**Configuring antivirus scanning for FS8600 with FluidFS v4**

Before you configure antivirus scanning, you may want to understand [How does FluidFS antivirus protect](#) data.

See [Excluding files and directory paths from scans](#) and [Supported antivirus applications](#) for more information.

**Configuring antivirus scanning**

To perform antivirus scanning, you must add an anti-virus server and then enable antivirus scanning on a per SMB share basis.

**Adding a NAS antivirus server**

Add one or more antivirus servers. Dell recommends adding multiple antivirus servers to achieve high-availability of virus scanning, and reduce the latencies for file access. NAS antivirus allocates scanning operations to the antivirus servers to maximize the available scanning bandwidth. The fewer the available antivirus servers, the more time required to scan files.

**Prerequisites**

- The anti-virus server must be network accessible. Dell recommends that the server is located on the same subnet as the FluidFS cluster.
- The antivirus server must run a supported ICAP-enabled antivirus application such as Symantec Protection Engine.
- The antivirus server must be present and working. If no server is available, file access is denied to clients.

**Steps**

1. Click the **Storage view**.

2. In the **Storage** pane, select a FluidFS cluster.

3. Click the **System** tab.

4. In the **System** tab navigation pane, select **AntiVirus Hosts**.

5. In the right pane, click the **AntiVirus Hosts** tab.

6. Click **Add AntiVirus Scanner**. The **Add AntiVirus Scanner** dialog appears.

7. In the **Name** field, type the host name or IP address of the antivirus server.
8. In the **Port** field, type the port that the FluidFS cluster uses to connect to the antivirus server.

9. Click **OK**.

**Deleting an antivirus server**
Delete an antivirus server when it is no longer available.

**Prerequisites**
If you have only one antivirus server, you cannot delete that server until you first disable antivirus scanning on all SMB shares.

**Steps**
1. Click the **Storage view**.
2. In the **Storage** pane, select a FluidFS cluster.
3. Click the **System** tab.
4. In the **System** tab navigation pane, select **AntiVirus Hosts**.
5. In the right pane, click the **AntiVirus Hosts** tab.
6. Select an antivirus server and click **Delete**. The **Delete** dialog appears.
7. Click **OK**.

**Enabling antivirus scanning for a SMB share**
Antivirus scanning is enabled on a per SMB share basis.

**Prerequisites**
You must configure antivirus servers before enabling antivirus scanning for a SMB share.

**Steps**
1. Click the **Storage view**.
2. In the **Storage** pane, select a FluidFS cluster.
3. Click the **File System** tab.
4. In the **File System** tab navigation pane, select SMB shares.
5. In the right pane, select a SMB share and click **Edit Settings**. The **Edit Settings** dialog box appears.
6. On the left pane choose Virus Scan then select **Virus Scan** check box.
7. Select the **Virus Scan** check box.
8. (Optional) Configure the remaining antivirus scanning attributes as needed. These options are described in the online help.
   - To deny access to files larger than the specified antivirus scanning file size threshold, select the **Deny un-scanned large files** check box.
• To change the maximum size of files that are included in antivirus scanning, type a size in the Anti-Virus Large File Size field in kilobytes (KB), megabytes (MB), gigabytes (GB), or terabytes (TB).

• To exempt file extensions from antivirus scanning, select the Enable virus scan extension exclusion check box and specify the extensions in the Extensions excluded from scan list.

• To exempt directories from antivirus scanning, select the Enable virus scan directory exclusion check box and specify the directories in the Directories excluded from scan list.

9. Click OK.

Allowing or denying access to files larger than the antivirus scanning file size threshold for a SMB share
Specify whether to allow or deny access to files that are larger than the specified antivirus scanning file size threshold for a SMB share.

1. Click the Storage view.

2. In the Storage pane, select a FluidFS cluster.

3. Click the File System tab.

4. In the File System tab navigation pane, select SMB shares.

5. In the right pane, select a SMB share and click Edit Settings. The Edit Settings dialog box appears, go to Virus scan on the right pane.

6. Allow or deny access to files larger than the antivirus scanning file size threshold.

   • To allow access to files larger than the antivirus scanning file size threshold, clear the Deny un-scanned large files check box.

   • To deny access to files larger than the antivirus scanning file size threshold, select the Deny un-scanned large files check box.

7. Click OK.

Changing the antivirus scanning file size threshold for a SMB share
Change the maximum size of files that are included in antivirus scanning for a SMB share.

1. Click the Storage view.

2. In the Storage pane, select a FluidFS cluster.

3. Click the File System tab.

4. In the File System tab navigation pane, select SMB shares.

5. In the right pane, select a SMB share and click Edit Settings. The Edit Settings dialog box appears, go to Virus scan on the right pane.
6. In the **Anti-Virus Large File Size** field, type a file size in kilobytes (KB), megabytes (MB), gigabytes (GB), or terabytes (TB).

7. Click **OK**.

**Including or excluding file extensions and directories in antivirus scanning for a SMB share**

Specify whether to perform antivirus scanning for all file extensions and directories for a SMB share, or exempt some file extensions and directories from antivirus scanning.

1. Click the **Storage** view.

2. In the **Storage** pane, select a FluidFS cluster.

3. Click the **File System** tab.

4. In the **File System** tab navigation pane, select SMB shares.

5. In the right pane, select a SMB share and click **Edit Settings**. The **Edit Settings** dialog box appears, go to Virus scan on the right pane.

6. Specify whether to perform antivirus scanning for all file extensions or exempt the specified file extensions from antivirus scanning.

   - **To perform antivirus scanning for all file extensions**, clear the **Enable virus scan extension exclusion** check box.
   
   - **To exempt the specified file extensions from antivirus scanning**, select the **Enable virus scan extension exclusion** check box.

7. **To specify file extensions to exempt from antivirus scanning**, add or remove file extensions in the antivirus scanning exemption list.

   - **To add a file extension to the antivirus scanning exemption list**, type a file extension (for example, docx) in the **Extensions excluded from scan** text field and click **Add**.

   - **To remove a file extension from the antivirus scanning exemption list**, select a file extension and click **Remove**.

8. Specify whether to perform antivirus scanning for all directories or exempt the specified directories from antivirus scanning.

   - **To perform antivirus scanning for all directories**, clear the **Enable virus scan directory exclusion** check box.

   - **To exempt the specified directories from antivirus scanning**, select the **Enable virus scan directory exclusion** check box.

9. **To specify directories to exempt from antivirus scanning**, add or remove directories in the antivirus scanning exemption list.

   - **To add a directory to the antivirus scanning exemption list**, type a directory (for example, /folder/subfolder) in the **Directories excluded from scan** text field and click **Add**.
• To remove a directory from the antivirus scanning exemption list, select a directory and click **Remove**.

10. Click **OK**.

**Disabling antivirus scanning for a SMB share**
Antivirus scanning is disabled on a per SMB share basis.

1. Click the **Storage** view.

2. In the **Storage** pane, select a FluidFS cluster.

3. Click the **File System** tab.

4. In the **File System** tab navigation pane, select **SMB shares**.

5. In the right pane, select a SMB share and click **Edit Settings**. The **Edit Settings** dialog box appears, go to Virus scan on the right pane

6. Clear the **Virus Scan** check box.

7. Click **OK**.

**Viewing antivirus events**

1. Events related to antivirus scanning can be viewed using Enterprise Manager.

2. Click the **Storage** view.

3. In the **Storage** pane, select a FluidFS cluster.

4. Click the **System** tab.

5. In the **System tab** navigation pane, select **AntiVirus Hosts**.

6. In the right pane, click the **Events** tab. The antivirus scanning events are displayed.

**Appendix**

**Excluding files and directory paths from scans**
You can control what files and directory paths are scanned as follows:

• Extensions excluded from scan: Specifies file extensions (file types) to exclude from scanning, such as .docx.

• Directories excluded from scan: Specifies directory paths to exclude from scanning, such as /tmp/logs (alternatively, folders and sub-folders).

The wildcards * (asterisk) and ? (question mark) are permitted when specifying directory paths, such as /user/*/tmp or /user/t?p.

**Supported antivirus applications**
For the latest list of supported antivirus applications, see the *Dell Fluid File System Version 4 Support Matrix*. 