Quest

Quest® Change Auditor for Fluid File System® 7.2

User Guide

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc.
Attn: LEGAL Dept.
4 Polaris Way
Aliso Viejo, CA 92656

Refer to our website (https://www.quest.com) for regional and international office information.

Patents

Quest Software is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at https://www.quest.com/legal.

Trademarks

Quest, the Quest logo, and Join the Innovation are trademarks and registered trademarks of Quest Software Inc. For a complete list of Quest marks, visit https://www.quest.com/legal/trademark-information.aspx. All other trademarks and registered trademarks are property of their respective owners.

Legend

CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

IMPORTANT NOTE, **NOTE**, **TIP**, **MOBILE**, or **VIDEO:** An information icon indicates supporting information.

Change Auditor for Fluid File System User Guide
Updated - January 2022
Software Version - 7.2

Contents

1

Change Auditor for Fluid File System Overview

Introduction

Change Auditor for Fluid File System tracks, audits, reports and alerts on file and folder changes in real time, translating events into simple text and eliminating the time and complexity required by system provided auditing. You can set the auditing scope on an individual file or folder or an entire file system recursive or non-recursive. You can include or exclude certain files or folders from the audit scope in order to ensure a faster and more efficient audit process.

Change Auditor for Fluid File System captures events and provides detailed information relating to the following activities:

- File and folder access
- File and folder creation, deletion and renames
- File and folder permission changes
- Content changes, such as file opens and writes

NOTE: Change Auditor for Fluid File System audits only SMB operations on FluidFS clusters.

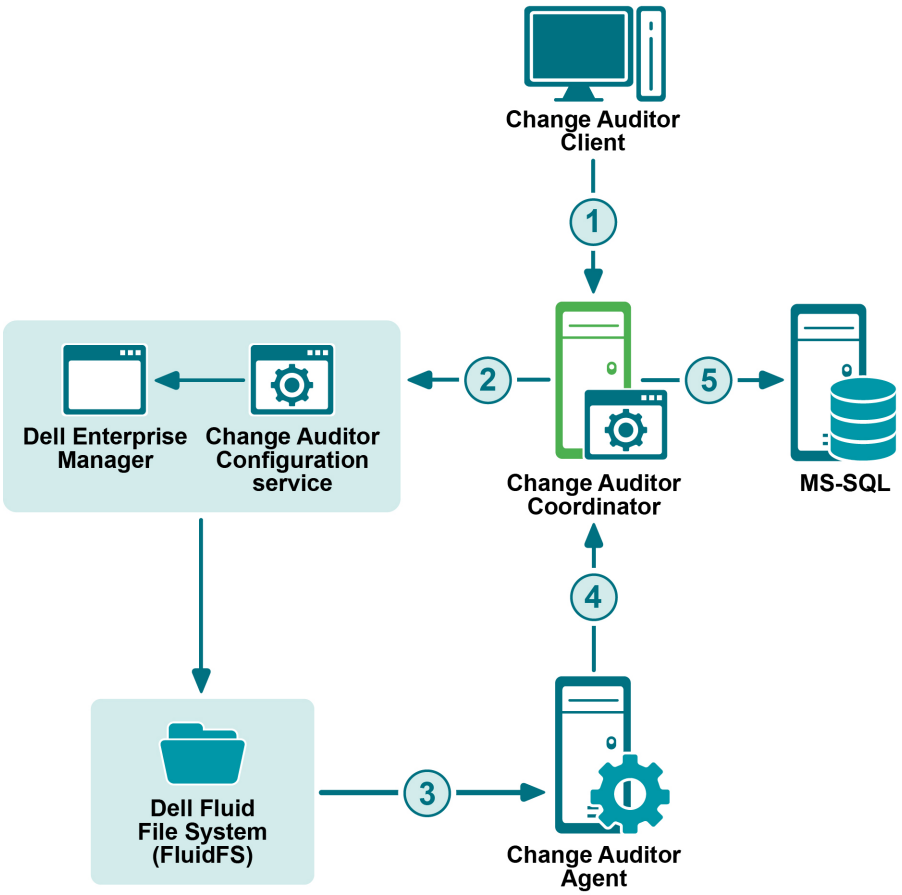
This guide has been prepared to assist you in becoming familiar with Change Auditor for Fluid File System. It is intended for network administrators, consultants, analysts, and any other IT professionals using the product.

- For information on the core functionality available in Change Auditor regardless of the product license that has been applied, see the Change Auditor User Guide and the Change Auditor Installation Guide.
- For event details, see the Change Auditor for Fluid File System Event Reference Guide.

System overview

The following details how Dell Fluid File System integrates with Change Auditor to provide auditing capability.

1. Using the Change Auditor client, users create a FluidFS auditing template to specify the FluidFS cluster, auditing settings, and the agents that are to receive the events. The client passes these settings to the coordinator for configuration.
2. The coordinator configures the FluidFS cluster through the Change Auditor Configuration Service for Dell FluidFS and Dell Enterprise Manager.
3. The FluidFS cluster forwards detailed information about the changes and activities back to the Change Auditor agent.
4. The agent captures events based on the auditing scope defined in the FluidFS auditing template and forwards them on to the coordinator.
5. The coordinator then forwards the events and related details to the Change Auditor database.



Deployment requirements

For a successful deployment, ensure that your environment meets the minimum system requirements. For information on system requirements, see the Change Auditor Release Notes. For installation details, see the Change Auditor Installation Guide.

Client components and features

The following table lists the client components and features that require a valid Change Auditor for Fluid File System license. The product will not prevent you from using these features; however, associated events will not be captured unless the proper license is applied.

NOTE: To hide unlicensed Change Auditor features from the Administration Tasks tab (including unavailable audit events throughout the client), use the **Action | Hide Unlicensed Components** menu command. Note this command is only available when the Administration Tasks tab is the active page.

Table 1. Change Auditor for Fluid File System client components/features

Client page	Feature
Administration Tasks Tab	Agent Configuration Page: • Event Logging - enable/disable FluidFS event logging **NOTE:** See FluidFS event logging for information on enabling FluidFS event logging. Audit Task List: • Fluid FS **NOTE:** See FluidFS Auditing for information on creating templates to define FluidFS auditing.
Event Details Pane	What Details: • Path • Attribute • Action
Events	Facilities: • FluidFS
Search Properties	What Tab: • Subsystem | File System **NOTE:** See Create custom FluidFS searches for information on using the What tab to create custom search queries.
Searches Page	Built-in Reports: • Report that include FluidFS events

2

Installation and configuration

Before you begin

Quest recommends that you perform the following steps before you begin the installation procedure:

- Review the complete installation process.
- Read the Change Auditor Release Notes for updated information.
- Ensure you have the appropriate license file to enable Change Auditor for FluidFS.

NOTE: For detailed instructions and required permissions for installing Change Auditor, see the Change Auditor Installation Guide.

Ensure Dell Fluid File System is properly installed and configured

NOTE: This guide only outlines the installation steps that are required in order for Change Auditor for Fluid File System to integrate with Dell Fluid File System.

- Verify that Dell Enterprise Manager Data Collector service and Dell Enterprise Manager Client are properly installed and configured.
- Verify that the FluidFS cluster you plan to audit is registered with Enterprise Manager.
- Ensure you have Administrator rights to Enterprise Manager.

Install the Change Auditor Configuration Service for Dell FluidFS

The Change Auditor Configuration Service for Dell FluidFS must be installed before you can audit FluidFS clusters.

IMPORTANT: The domain of the configuration service must have a two-way trust with the domain of the auditing agent and trust the domain of the coordinator (one-way trust).

NOTE: Ensure that Windows PowerShell version 4 is installed on the computer where the configuration service is installed.

NOTE: The service requires x64 version of Microsoft's .NET 4.5.2.

To install the service

1. Run the Change Auditor Configuration Service for Dell FluidFS.msi which is located in the Integration/FluidFS folder of the installation package.
2. Read the welcome message and click **Next** to continue or **Cancel** to exit.
3. Accept the license agreement and click **Next**.
4. Enter the required Enterprise Manager server and click **Install**.
5. Click **Finish** to complete the installation and exit the wizard.

If you need to change the Enterprise Manager server address after it has been installed

1. Open the FluidFS.Configuration.Service.exe.config file. The default location for this file is "C:\Program Files\Quest\ChangeAuditor\FluidFS Configuration Service" where the FluidFS Configuration service is installed.
2. Edit the Enterprise Manager server address with the following snippet in the code:

```
<appSettings>
   <add key="ServicePort" value="9003"/>
   <add key="EnterpriseManagerServer" value="[IP/NetBIOS/FQDN address]"/>
</appSettings>
```

3. Restart the Change Auditor Configuration Service for Dell FluidFS in the Service Control Manager.

3

Getting Started

Deployment requirements

You can search, report and alert on changes to a specific volume or all volumes on a FluidFS NAS and receive real-time alerts whenever someone tries to access a secure file, folder or volume on a FluidFS cluster.

Before you can begin to capture FluidFS activity events, you must:

- Ensure you meet the minimum system requirements.
- Apply the ChangeAuditor for FluidFS license.
- Deploy agents to monitor cluster volumes. See the Change Auditor Installation Guide for more information on deploying agents.
- Create FluidFS templates. See FluidFS Auditing for details on creating templates.

This section provides a high-level view of the tasks to get you started using Change Auditor for FluidFS.

NOTE: FluidFS auditing is only available if you have licensed Change Auditor for Fluid File System. If you do not have a valid license you can use the features, however, associated events are not captured. To verify that it is licensed, right-click the coordinator icon in the system tray and select **Licensing.**

Verify auditing template is applied

To ensure FluidFS events are being captured, check to see if the Change Auditor agent assigned to the FluidFS auditing template is using the latest agent configuration.

To verify that latest agent configuration is being used:

1. Select **Start | All Programs | Quest | Change Auditor | Change Auditor Client**.
2. Open the Administration Tasks tab (**View | Administration** menu command).
3. If not already selected, click **Configuration**.
4. Select **Agent** in the Configuration task list to open the Agent Configuration page.
5. Select the Change Auditor agent assigned to the FluidFS Auditing template (**Auditing** appears in the **FluidFS** column) and click **Refresh Configuration**.

Make changes and run a report

1 To test FluidFS auditing, make some changes to the FluidFS cluster being monitored.

For example:

- create a new folder
- add a new .txt or .docx file in this folder
- delete the sample .txt file
- add a sub-folder
- change the security permission of the new folder

2 Select **Start | All Programs | Quest | Change Auditor | Change Auditor Client**.

3 Open the Searches tab.

4 Expand the **Shared | Built-in | All Events** folder in the left-hand pane.

5 Locate and double-click **All FluidFS Events** in the right-hand pane.

A new Search Results tab is added to the client displaying the FluidFS events that were captured.

6 Select an event from the Search Results grid to display the event details for the selected event.

NOTE: If the Search Properties tabs are displayed across the bottom of the Search Results page, double-click an event to display the event details for the selected event.

4

FluidFS Auditing

Introduction

You must define a FluidFS Auditing template for each cluster to audit. The FluidFS Auditing page on the Administration Tasks tab displays details about each template created and allows you to add new auditing templates.

This section provides a description of the FluidFS Auditing page and Auditing wizard which walks you through the process of creating a new auditing template. It also explains the File System Event settings available on the Configuration Setup dialog which can be used to define how to process duplicate File System events. For a description of the dialogs mentioned in this chapter, refer to the online help. For more information about agent configurations, refer to the Change Auditor User Guide.

FluidFS Auditing page

The FluidFS Auditing page displays when you select **FluidFS** from the Auditing task list in the navigation pane of the Administration Tasks tab. From this page you can launch the FluidFS Auditing wizard to specify the FluidFS cluster to be audited, the auditing scope, and the agents that are to receive the events. You can also edit existing templates, disable/enable templates, and remove templates that are no longer being used.

NOTE: Authorization to use the administration tasks on the Administrations Tasks tab is defined using the Application User Interface page under the Configuration task list. If you are denied access to the tasks on this page, refer to the Change Auditor User Guide for more information on how to gain access.

The FluidSFS Auditing page contains an expandable view of all the templates that have been previously defined. To add a new template to this list, use the **Add** tool bar button. Once added, the following information is provided for each template:

Volume

Displays the name of the FluidFS volume specified in the wizard.

Status

Indicates whether the auditing template is enabled or disabled.

Include Mask

Displays the names of the subfolders or files to be audited (or a file mask) as specified on the Inclusions tab of the wizard.

Excludes

Displays the names and paths of subfolders and files to be excluded from auditing as specified on the Exclusions tab of the wizard.

Operations

Displays the events selected for auditing on the Events tab of the wizard. Hover your mouse over this cell to view all of the events included in the template.

Agent

Lists the Change Auditor agents assigned to receive the events from the selected cluster.

FluidFS Auditing templates

To enable FluidFS auditing, you must first create an auditing template for each cluster to audit. Each auditing template defines the location of the cluster to be audited, the auditing scope, and the agents that are to receive the events.

NOTE: There can be only one FluidFS auditing template per cluster. If you want to audit multiple audit paths, use the same template to specify all the audit paths to be audited on the selected cluster.

To audit a volume:

1. Create a FluidFS auditing template. See FluidFS Auditing wizard for details.

   Once you have configured your template, the associated event notifications will be set in Enterprise Manager. (Within Enterprise Manager, right-click the volume and select **Edit File Access Notification**).
2. On the Administration Tasks tab, click **Configuration** and select **Agent** in the Configuration task list to open the Agent Configuration page.
3. Select the Change Auditor agents assigned to the FluidFS template and click **Refresh Configuration** to ensure the agents are using the latest configuration.

   NOTE: If you do not refresh the agent's configuration, the agent will automatically check for a new agent configuration based on the polling interval setting (located on the System Settings tab of the Configuration Setup dialog). The default is every 15 minutes.

To disable an auditing template:

The disable feature allows you to temporarily stop auditing the specified volume without having to remove the auditing template or individual volume from a template.

1. On the Auditing page, use one of the following methods to disable an auditing template:
   - Place your cursor in the **Status** cell for the template to be disabled, click the arrow control and select **Disabled**.
   - Right-click the template to be disabled and select **Disable**.

   The entry in the **Status** column for the template will change to 'Disabled'.
2. To re-enable the auditing template, use the **Enable** option in either the **Status** cell or right-click menu.

To delete an auditing template:

1. On the Auditing page, select the template to be deleted and click the **Delete | Delete Template** tool bar button.
2. A dialog will be displayed confirming that you want to delete the selected template. Click **Yes**.

NOTE: To delete the template when a connection cannot be made with the FluidFS cluster, use the Clear-CAFluidFSTemplate command. Auditing settings must be removed from the cluster using Enterprise Manager.

FluidFS Auditing wizard

The FluidFS Auditing wizard displays when you click the **Add** tool bar button on the FluidFS Auditing page. This wizard steps you through creating a new FluidFS auditing template, specifying the volume to audit, and configuring the agents to receive the events.

The following table provides a description of the fields and controls in the FluidFS Auditing wizard.

NOTE: A red flashing icon indicates that you have not yet entered the required information. Hovering your cursor over this icon displays a tool tip explaining what needs to be entered. A green check mark indicates that the required information has been specified and you are ready to proceed.

Table 2. FluidFS Auditing wizard

Create or modify a FluidFS Auditing Template page: On the first page of the wizard, specify the FluidFS cluster to audit and define the auditing scope.	
FluidFS cluster	Enter or select the FluidFS cluster from the drop-down list to be audited. **NOTE:** IP Addresses are not supported at this time. **NOTE:** The drop-down list contains the clusters published in Active Directory.
Volume	To select or enter a volume to be audited, you must enter the Change Auditor Configuration Service for Dell FluidFS location and an account that has administrative privileges to access Enterprise Manager. This allows the Coordinator to connect with the service and populate the list of available volumes to audit. The credentials are case sensitive.
Add	Use to move the volume to the selection list.
Remove	Select an entry in the selection list and click **Remove** to remove it from the list.
Events tab	Use the Events tab to select vital file and/or folder events.
File Events	Select the file events to audit. Select the **File Events** check box to select all of the file events listed or select individual events from the list.
Folder Events	Select the folder events to audit. Select the **Folder Events** check box to select all of the folder events listed or select individual events from the list.
Inclusions tab	Use the Inclusions tab to specify what in the selected volume will be audited.
Add the names of subfolders and files to audit	Enter a file mask to specify what in the volume to audit. The file mask can contain any combination of the following: • Fixed characters such as letters, numbers and other characters that are allowed in file names. • Asterisk (*) wildcard character to substitute zero or more characters. • Question mark (?) wildcard character to substitute a single character. • A double asterisk (**) to specify a recursive match. (find match in the folder and all subfolders in audit path). For example, entering * will include all folders and files in the selected audit path. See File/Folder Inclusion and Exclusion Examples for more file mask examples. You can also enter the name of an individual subfolder or file that is to be included. However, if you enter the name of a subfolder, you will only receive events for operations performed against the specified subfolder. You will NOT receive events for operations performed against any child objects under the specified subfolder. Once you have specified the subfolders or files to be included, click **Add** to add it to the Inclusions list.

Table 2. FluidFS Auditing wizard

Inclusions list	The list across the bottom of this page contains the subfolders and files selected for auditing. Use the buttons to the right of the text box to add and remove entries.
Add	Use to move the entry in the text box to the Inclusions list.
Remove	Select an entry in the Inclusions list and click **Remove** to remove it.
Exclusions Tab (Optional)	The Exclusions tab allows you to refine the settings defined on the Inclusions tab. That is, you can optionally specify the names and paths of any subfolders and files in the selected volume to exclude from auditing.
NOTE: To reduce the number of events generated by document File | Save operations in Microsoft Word, Excel, Visio, and PowerPoint (Microsoft Office version 2010, 2013, and 2016), Change Auditor uses event consolidation rules. Excluding temporary files will remove the ability to consolidate these events and you will lose file modified events. Consolidation rules are not supported in multiple agent auditing scenarios.	
Add the names and paths of subfolders and files to exclude from auditing	Enter a file mask to specify the name and path of subfolders and files to be excluded from auditing. The file mask can contain any combination of the following: • Fixed characters such as letters, numbers and other characters that are allowed in file names. • Asterisk (*) wildcard character to substitute zero or more characters. Use a single asterisk (*) to specify a non-recursive match (i.e., find match in the folder only; does not match any slash characters (\)). Use a double asterisk (**) to specify a recursive match (i.e., find match in the folder and all subfolders in audit path; matches slash characters (\) and directory names in paths). • Question mark (?) wildcard character to substitute a single character. The ? wildcard character does not match slash (\) characters. For example, entering ***.log** will exclude all files in the audit folder with the .log file extension. Whereas, entering ****.log** will exclude all files with the .log file extension found in the audit folder or in any subfolders. See File/Folder Inclusion and Exclusion Examples for more examples. You can also enter the name of an individual subfolder or file that is to be excluded from auditing. **IMPORTANT:** If you enter the name of a subfolder or file that is outside of the audited path, Change Auditor will NOT exclude it from auditing. Once you have selected a subfolder or file to be excluded, select the appropriate **Add** button to add it to the Exclusions list.
Exclusions list	The list across the bottom of this page contains the folders, files and masks that are to be excluded from auditing. Use the buttons to the right of the text box to add and remove entries.
Add	Use one of the following **Add** commands to move the entry in the text box to the Exclusions list: • **Add | Folder** - use this option to exclude activity against files/subfolders in any folders that match the exclusion string. • **Add | File** - use this option to exclude activity against any files that match the exclusion string.
Remove	Select an entry in the Exclusions list and click **Remove** to remove it.

Table 2. FluidFS Auditing wizard

Select Change Auditor agents page: Use this page to select the Change Auditor agents that are to receive the events captured on the selected FluidFS cluster.

NOTE: The domain of the configuration service must have a two-way trust with the domain of the auditing agent and trust the domain of the coordinator (one-way trust).

NOTE: You may improve performance by assigning an auditing template to more than one Change Auditor agent. When multiple agents are assigned to the same template, events will be load balanced between these agents. However, the downside is that the 'where' field for events may contain any one of the agents being monitored by this single auditing template. In addition, if FluidFS event logging is enabled in Change Auditor, events will be written on multiple agent servers.

Add	Click **Add** to assign one or more Change Auditor agents to the FluidFS auditing template. Selecting this button displays the eligible Change Auditor Agents dialog. From this dialog, select one or more agents and then click **OK**.
Remove	Click **Remove** to remove the selected agent from the list.
Change Auditor Agent list	The list across the bottom of the page lists the Change Auditor agents selected to capture events from the selected FluidFS cluster.
(Optional) Encryption settings page:	Turn encryption on to protect the data as it passes between the FluidFS cluster and the agents.
Refresh status	Click **Refresh status** to see the encryption status.
Turn on encryption for auditing	To enable encryption, select **Turn on encryption for auditing**, click the **Set credentials for encryption**, and enter the service account credentials for the FluidFS cluster to use when encrypting events. **NOTE:** The domain of the coordinator must trust the domain of the specified user account (one-way trust). **NOTE:** When required, you can turn off the encryption through the Enterprise Manager client. If you turn off encryption, you need to refresh Change Auditors' configuration so that it is synchronized with the FluidFS cluster. To refresh the configuration, save the FluidFS template after the change or run the UpdateCAFluidFSConfiguration PowerShell command found in the installation directory of the Change Auditor Configuration Service for Dell FluidFS. **NOTE:** Encryption settings are not maintained when a template is exported. You will need to re-configure this setting on any previously deleted templates after it has been imported.

NOTE: To reduce the number of events generated by document File | Save operations in Microsoft Word, Excel, Visio, and PowerPoint, Change Auditor uses event consolidation rules. Excluding .tmp files will remove the ability to consolidate these events and you will lose file modified events.

FluidFS event logging

In addition to real-time event auditing, you can enable event logging to capture FluidFS events locally in a Windows event log. This event log can then be collected using InTrust™ to satisfy long-term storage requirements.

Event logging is disabled by default. When enabled, only configured activities are sent to the Change Auditor for FluidFS event log. See the Change Auditor for Fluid File System Event Reference Guide for a list of the events that can be sent to the event log.

To enable event logging:

1. Open the Administration Tasks tab.
2. Click **Configuration**.
3. Select **Agent** in the Configuration task list to display the Agent Configuration page.
4. Click the **Event Logging** tool bar button.
5. On the Event Logging dialog, select **FluidFS**.
6. Click **OK** to save your selection and close the dialog.

   The events configured in the FluidFS Auditing template will then be sent to the Change Auditor for FluidFS event log.

5

FluidFS Searches/Reports

Introduction

Change Auditor provides built-in searches that can be run to retrieve FluidFS activity captured by deployed agents enabling you to retrieve valuable information from a variety of perspectives.

NOTE: The terms ‘searches’ and ‘reports’ are used in conjunction to acquire the desired output. You run a ‘search’ and the results returned are referred to as a ‘report’.

You to create custom search definitions to search for file and/or folder changes to a specific volume. You will use the Search Properties tabs across the bottom of the Searches page to define new custom searches.

This section explains how to run a built-in search and create custom searches. For a description of the dialogs mentioned in this chapter, please refer to the online help. For a description of the Search Properties tabs and how to use these tabs to customize your searches, see the Change Auditor User Guide.

FluidFS built-in searches

This section provides procedures for running built-in searches and provides a description of the details displayed on the Search Results page for FluidFS events.

To see a complete list of built-in reports, see the Change Auditor Built-in Reports Reference Guide.

To run a built-in search:

1. Click on the **Searches** tab.
2. Select **Shared | Built-in | All Events** to display the list of search definitions stored in the selected folder.
3. In the right-hand pane, locate the All FluidFS and click **Run**
4. A new Search Results Page will be displayed populated with the audited events that met the search criteria defined in the selected search definition.

NOTE: To modify a built-in search, see the Change Auditor User Guide.

Create custom FluidFS searches

The following scenarios explain how to use the What tab to create custom FluidFS searches.

NOTE: If you wanted to, you can use the other search properties tabs to define additional criteria:

- Who - allows you to search for events generated by a specific user, computer or group
- Where - allows you to search for events captured by a specific agent or within a specific domain or site
- When - allows you to search for events that occurred within a specific date/time range
- Origin - allows you to search for events that originated from a specific workstation or server

To search for all file system events including FluidFS events:

1 Open the Searches page.

2 In the explorer view (left pane), expand and select the folder where you want to save your search.

Selecting the **Private** folder will create a search that only you can run and view, whereas selecting the **Shared** folder will create a search which can be run and viewed by all Change Auditor users.

3 Click **New**.

This enables the Search Properties tabs across the bottom of the Searches page.

4 On the Info tab, enter a name and description for the search.

5 Open the What tab, expand **Add** and select **Subsystem | File System**.

6 On the Add File System Path dialog, select the **All File System Paths** option.

7 Review the Actions section and select those that are to be included in the search.

By default, **All Actions** is selected meaning that all of the actions associated with the file system path will be included in the search.

8 Click **OK** to save your selection and close the dialog.

9 Once you have defined your search criteria, click **Run** to save and run the search.

10 When this search runs, Change Auditor searches for all file system events including FluidFS events and display the results in a new search results page.

To search for events performed against a specific FluidFS file or folder:

1 Open the Searches page.

2 In the explorer view (left pane), expand and select the folder where you want to save your search.

Selecting the **Private** folder will create a search that only you can run and view, whereas selecting the **Shared** folder will create a search which can be run and viewed by all users.

3 Click **New**.

This will activate the Search Properties tabs across the bottom of the Searches page.

4 On the Info tab, enter a name and description for the search.

5 Open the What tab, expand **Add** and select **Subsystem | File System**.

6 On the Add File System Path dialog, select one of the following scope options:

- **This Object** - select to search only the selected object.
- **This Object and Child Objects Only** - select to search the selected object and its direct child objects.
- **This Object and All Child Objects** - select to include the selected object and all subordinate objects (in all levels)

7 In the **Path** field, enter or use the browse button to select the FluidFS path to be searched.

To search for events against a specific volume, enter the path as follows: \\<*VolumeName*>

To search for events against a specific folder, enter the path as follows: \\<*VolumeName*>\<*FolderName*>\

To search for events against a specific file, enter the path as follows:
\\<*VolumeName*>\<*FolderName*>\<*FileName*>

> **NOTE:** If the scope of your search is **This Object**, you can use the * wildcard character to specify the FluidFS path. That is, use an asterisk (*) to substitute zero or more characters.
>
> When using the **This Object** option, be sure to select the appropriate **Type** option to define the type of path to be searched: **Files** or **Folders**.

8 Review the Actions section and select those that are to be included in the search.

By default, **All Actions** is selected meaning that all of the actions associated with the path will be included in the search.

When the scope includes child objects, **All Types** are selected by default meaning that all types of paths will be searched. If you selected the **This Object** scope option, **Files** is selected by default, which can be changed to **Folders**. Only one type can be selected.

> **NOTE:** The Transaction option does not apply to FluidFS events.

9 Click **OK** to save your selection and close the dialog.

10 Click **Run** to save and run the search. Click **Save** to save the search definition without running it.

11 When this search runs, Change Auditor searches for FluidFS events in the selected path and display the results in a new search results page.

To search for a specific FluidFS event class:

1 Open the Searches page.

2 In the explorer view (left pane), expand and select the folder where you want to save your search.

Selecting the **Private** folder will create a search that only you can run and view, whereas selecting the **Shared** folder will create a search which can be run and viewed by all Change Auditor users.

3 Click **New**.

This enables the Search Properties tabs across the bottom of the Searches page.

4 On the Info tab, enter a name and description for the search.

5 Open the What tab, click **Add** (or expand the **Add** tool bar button and select **Event Class**).

6 On the Add Facilities or Event Classes dialog, enter **FluidFS** in the filter field under the Facility heading to display all of the FluidFS events.

7 From this list, select one or more events and use the **Add | Add This Event** option to add the selected events to the list box at the bottom of the dialog. Click **OK** to save your selection and close the dialog.

8 Click **Run** to save and run the search. Click **Save** to save the search definition without running it.

9 When the search runs, Change Auditor searches for the FluidFS events based on the search criteria specified on the What tab and display the results in a new search results page.

6

FluidFS Events

The following events can be selected for auditing from the Events tab on the FluidFS Auditing wizard. For details and the available built-in searches see the Change Auditor for Fluid File System Event Reference Guide.

File events

- FluidFS File auditing changed
- FluidFS File created
- FluidFS File deleted
- FluidFS File moved
- FluidFS File renamed
- FluidFS File opened
- FluidFS File ownership changed
- FluidFS File access rights changed
- FluidFS File contents written

Folder events

- FluidFS Folder auditing changed
- FluidFS Folder created
- FluidFS Folder deleted
- FluidFS Folder moved
- FluidFS Folder renamed
- FluidFS Folder ownership changed
- FluidFS Folder access rights changed

7

File/Folder Inclusion and Exclusion Examples

This section provides sample entries for the Inclusions and Exclusions tabs on the auditing wizard. It does not list every combination available, but provides a variety of examples to help you understand how to use the wildcard characters allowed on these two tabs.

Use these two tabs as described below:

- Inclusions tab - enter a file mask to specify what is to be audited.
- Exclusions tab - optionally enter a file mask (or path) to specify subfolders and files in the selected audit path that are to be excluded from auditing.

Inclusions tab

You must enter a file mask on the Inclusions tab to specify what is to be audited in the selected audit path. Use the following characters to specify a file mask on the Inclusions tab:

- Fixed characters such as letters, numbers and other characters that are allowed in file names.
- An asterisk (*) wildcard character to substitute zero or more characters.
- Question mark (?) wildcard character to substitute a single character.
- A double asterisk (**) to specify a recursive match. (find match in the folder and all subfolders in audit path).

Examples:

The following table provides some examples of file masks that can be used on the Inclusions tab of the auditing wizard. Note that <*String*> in this table may contain any of the file mask characters described above (i.e., fixed characters, * or ?).

Table 3. Inclusion examples

What is included in the audit:	Inclusion syntax/examples:
Include all files located anywhere in the audit path. **NOTE:** This is the most commonly used file mask.	**Inclusion Syntax:** *
Include all files with a specific file name regardless of its file extension.	**Inclusion Syntax:** <*FileName*>.* **Example:** Name.* **Includes:** Name.txt Name.docx Name.pdf

Table 3. Inclusion examples

What is included in the audit:	Inclusion syntax/examples:
Include all files with a specific file extension.	**Inclusion Syntax:** <*FileNameString*>.<*Ext*> **Example 1:** *.tmp **Includes:** Files with a file extension of .tmp. Name.tmp Testing.tmp **Example 2:** ???*.doc **Includes:** Files whose name contains at least three characters with a file extension of .doc. MyTest.doc Testing123.doc 123.doc **Example 3:** ???test.doc **Includes:** Files whose name contains seven characters and ends in 'test' with a file extension of .doc. ABCtest.doc 123test.doc
Include all files with a specific file name that has a file extension of a specific length (number of characters).	**Inclusion Syntax:** <*FileName*>.<*ExtString*> **Example 1:** Name.??? **Includes:** Name.txt Name.tmp Name.pdf **Example 2:** Name.???? **Includes:** Name.docx Name.xlsx
Include all files that contain a specific string in their name and/or file extension.	**Inclusion Syntax:** <*FileNameString*>.<*ExtString*> **Example:** *name.??p **Includes:** Files whose name end with 'name' with a three character file extension that ends in the letter 'p'. Myname.tmp Name.bmp

Exclusions tab

If you do not want to exclude anything (folders or files) in the audit path from auditing, skip this tab. However, if you want to exclude a specific folder/file or group of folders/files, use the following characters to specify what is to be excluded:

- Fixed characters such as letters, numbers and other characters that are allowed in file names.
- An asterisk (*) wildcard character to substitute zero or more characters.

  NOTE: Use a single asterisk (*) to specify a non-recursive match (find match in the folder only; does not match any slash characters (\)).

  Use a double asterisk (**) to specify a recursive match (find match in the folder and all subfolders in audit path; matches slash characters (\) and directory names in paths).

- Question mark (?) wildcard character to substitute a single character (does not match any slash characters (\).

NOTE: Be sure to select the appropriate **Add** option (Folder or File) when adding an exclusion or you may not get the results expected. That is, use **Add | Folder** to exclude the auditing of activity against files/subfolders in folder(s) that match the exclusion string. Use **Add | File** to exclude the auditing of activity against file(s) that match the exclusion string.

Examples

The following tables provide some examples of file masks that can be used on the Exclusions tab of the auditing wizard. Note that <*String*> in these tables may contain any of the file mask characters described above (i.e., fixed characters, * or ?).

Audit Path = Volume (<VolumeName>)

In the following examples, the volume name is Vol0 (Audit Path = Vol0).

NOTE: Volume names are case sensitive and must be entered correctly in the **Audit Path** field on the auditing wizard.

Table 4. Exclusion examples: Audit Path = Volume

What to exclude:	Exclusion syntax/examples:
Exclude activity against files/subfolders in a specific folder found in a specific location on the selected volume. (**Add | Folder**)	**Exclusion Syntax:** <*Path*>\<*FolderName*> **Example:** HOME\USERS\TEMP\DOCS **Excludes:** Vol0\HOME\USERS\TEMP\DOCS
Exclude activity against files/subfolders in all folders whose name contains a specific string of characters found in a specific location on the selected volume. (**Add | Folder**)	**Exclusion Syntax:** <*Path*>\<*CharString*> **Example:** HOME\USERS\TE?????DOCS **Excludes:** Vol0\HOME\USERS\TESTINGDOCS Vol0\HOME\USERS\TEMPORARYDOCS
Exclude activity against files/subfolders in all folders with the specified folder name. (**Add | Folder**)	**Exclusion Syntax:** **\<*FolderName*> **Example:** HOME**\DOCS **Excludes:** Vol0\HOME\DOCS Vol0\HOME\DEPTS\DOCS Vol0\HOME\USERS\TEMP\DOCS

Table 4. Exclusion examples: Audit Path = Volume

What to exclude:	Exclusion syntax/examples:
Exclude activity against files/subfolders in all folders whose name starts with a specific string of characters. (**Add | Folder**)	**Exclusion Syntax:** **\<*CharString*>* **Example:** HOME**\DOC* **Excludes:** Vol0\HOME\DOCS Vol0\HOME\DEPTS\DOCS Vol0\HOME\USERS\TEMP\DOCS Vol0\HOME\USERS\DOCUMENTS
Exclude activity against files/subfolders in all folders with the specified folder name found in a specific path level on the selected volume. (**Add | Folder**)	**Exclusion Syntax:** **\<*FolderName*> **Example 1:** **\DOCS **Excludes:** Vol0\HOME\USERS\DOCS Vol0\HOME\DEPTS\DOCS Vol0\SHARE2\TEST\DOCS Example 2: ***\DOCS Excludes: Vol0\HOME\USERS\TEMP\DOCS Vol0\SHARE2\PUBLIC\TEST\DOCS
Exclude activity against files/subfolders in all folders with the specified folder name which may be located anywhere on the selected volume. (**Add | Folder**)	**Exclusion Syntax:** **\<*FolderName*> **Example:** **\DOCS **Excludes:** Vol0\HOME\DOCS Vol0\HOME\DEPTS\DOCS Vol0\HOME\USERS\TEMP\DOCS Vol0\TEST\DOCS Vol0\PUBLIC\TEST\DOCS
Exclude activity against files/subfolders in all shares and folders whose name contains a specific string of characters which may be located anywhere on the selected volume. (**Add | Folder**)	**Exclusion Syntax:** **<*CharString*>* **Example:** **DOC* **Excludes:** Vol0\HOME\DOCS Vol0\HOME\MYDOCS Vol0\HOME\USERS\TEMP\DOCS Vol0\HOME\USERS\TEMPORARYDOCS Vol0\TEST\DOCS Vol0\PUBLIC\TEST\MYDOCS Vol0\SHAREDDOC
Exclude activity against files whose name contains a specific string of characters which may be found anywhere on the selected volume. (**Add | File**)	**Exclusion Syntax:** **<*CharString*>* **Example:** **DOC* **Excludes:** Vol0\HOME\Document1.tmp Vol0\HOME\DOCS\Testing.doc Vol0\HOME\USERS\TEMP\DOCS\BetaDoc.pdf Vol0\USERS\DOCS\Test1.docx Vol0\PUBLIC\MYDOCS\OldDocPlan
Exclude activity against a specific file found in a specific location on the selected volume. (**Add | File**)	**Exclusion Syntax:** *<Path>\<FileName.Ext>* **Example:** USERS\DOCS\Test1.docx **Excludes:** Vol0\USERS\DOCS\Test1.docx

Table 4. Exclusion examples: Audit Path = Volume

What to exclude:	Exclusion syntax/examples:
Exclude activity against files with a specific file name (regardless of the file extension) which may be located anywhere on the selected volume. (**Add | File**)	**Exclusion Syntax:** **\<*FileName*>.* **Example:** **\test1.* **Excludes:** Vol0\HOME\DEPTS\DOCS\test1.docx Vol0\HOME\USERS\TEMP\DOCS\test1.docx Vol0\HOME\USERS\DOCUMENTS\test1.pdf Vol0\TEST\DOCS\test1.txt
Exclude activity against files with the specified file extension found in a specific location on the selected volume. (**Add | File**)	**Exclusion Syntax:** <*Path*>*.<*Ext*> **Example:** SHARE2\TEST\DOCS*.docx **Excludes:** Vol0\TEST\DOCS\Test1.docx Vol0\TEST\DOCS\MyInfo.docx
Exclude activity against files with the specified file extension which may be located anywhere on the selected volume. (**Add | File**)	**Exclusion Syntax:** ***.<*Ext*> **Example:** ***.pdf **Excludes:** Vol0\HOME\MYDOCS\Final.pdf Vol0\HOME\DEPTS\DOCS\Test123.pdf Vol0\HOME\USERS\DOCUMENTS\Test1.pdf Vol0\TEST\DOCS\Current.pdf Vol0\PUBLIC\TEST\MYDOCS\Ex.pdf

About us

Quest creates software solutions that make the benefits of new technology real in an increasingly complex IT landscape. From database and systems management, to Active Directory and Office 365 management, and cyber security resilience, Quest helps customers solve their next IT challenge now. Around the globe, more than 130,000 companies and 95% of the Fortune 500 count on Quest to deliver proactive management and monitoring for the next enterprise initiative, find the next solution for complex Microsoft challenges and stay ahead of the next threat. Quest Software. Where next meets now. For more information, visit www.quest.com.

Our brand, our vision. Together.

Our logo reflects our story: innovation, community and support. An important part of this story begins with the letter Q. It is a perfect circle, representing our commitment to technological precision and strength. The space in the Q itself symbolizes our need to add the missing piece—you—to the community, to the new Quest.

Contacting Quest

For sales or other inquiries, visit www.quest.com/contact.

Technical support resources

Technical support is available to Quest customers with a valid maintenance contract and customers who have trial versions. You can access the Quest Support Portal at https://support.quest.com.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request.
- View Knowledge Base articles.
- Sign up for product notifications.
- Download software and technical documentation.
- View how-to-videos.
- Engage in community discussions.
- Chat with support engineers online.
- View services to assist you with your product.