Quest

Quest® Change Auditor for Windows® File Servers 7.6.3

User Guide

© 2026 Quest Software Inc.

ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Quest Software Inc.

The information in this document is provided in connection with Quest Software products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Quest Software products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, QUEST SOFTWARE ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL QUEST SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF QUEST SOFTWARE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Quest Software makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Quest Software does not make any commitment to update the information contained in this document.

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

Quest Software Inc.
Attn: LEGAL Dept.
10801 N. Mopac Expressway
Building 3, Suite 400
Austin, TX 78759

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 Windows File Servers User Guide
Updated - August 2026
Software Version - 7.6.3

Contents

Change Auditor for Windows File Servers Overview 4
Introduction 4
Deployment requirements 4
Client components/features 4

Getting Started 6
Introduction 6
Getting started 6
Create File System Auditing template 7
Make File System changes and run a report 8
Troubleshooting steps 8

File System Auditing 10
Introduction 10
File System Auditing page 10
File System Auditing templates 12
File System Auditing wizard 17
File System Event settings 21
File System event logging 22

File System Searches/Reports 23
Introduction 23
Create custom File System search 23

File System Protection 25
Introduction 25
File System Protection page 25
File System Protection templates 27
File System Protection wizard 30

File System Events 34

File/Folder Inclusion and Exclusion Examples 36
Inclusions tab 36
Exclusions tab 38

About us 42
Our brand, our vision. Together. 42
Contacting Quest 42
Technical support resources 42

1

Change Auditor for Windows File Servers Overview

- Introduction
- Deployment requirements
- Client components/features

Introduction

Change Auditor for Windows File Server tracks, audits, and alerts on file and folder changes in real time, translating events into simple terms and eliminating the time and complexity required by system provided auditing. The auditing scope can be set 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 to ensure a faster and more efficient audit process.

In addition to File System auditing, you can protect and lock down critical file system paths from unauthorized or accidental modifications or deletions.

This guide has been prepared to assist you in becoming familiar with Change Auditor for Windows File Servers. 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 Windows File Servers Event Reference Guide.

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 details on installing Change Auditor, see the Change Auditor Installation Guide.

Client components/features

The following table lists the client components and features that require a valid Change Auditor for Windows File Servers license.

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

Table 1. Change Auditor for Windows File Servers client components/features

Client Page	Feature
Administration Tasks Tab	Agent Configuration Page: • Event Logging - enable/disable File System event logging • Configuration Setup Dialog - File System Tab ▪ Discard duplicates that occur within *nn* seconds ▪ Audit all configured, including duplicates (Not Recommended) Audit Task List: • File System **NOTE:** See File System Auditing for information on enabling event logging, viewing/modifying the agent configuration settings and on creating templates to define File System auditing. Protection Task List: • File System **NOTE:** See File System Protection for information on creating File System protection templates.
Event Details Pane	What Details: • Path • Attribute • Process
Events	Facilities: • Custom File System Monitoring
Search Properties	What Tab: • Subsystem | File System **NOTE:** See File System Searches/Reports for information on using the What tab to create custom File System search queries.
Searches Page	Built-in Reports: • Reports that include Custom File System Monitoring events.
Alert Body Configuration Dialog - Event Details Tab	Variables (email tags): • FS_ATTRIBUTENAME • FS_FILENAME • FS_FILESERVER • FS_FILESYSTEMTYPEID • FS_FOLDERPATH • FS_LOGONID • FS_PRIMARYSID • FS_PROCESSNAME • FS_SHARENAME • FS_TRANSCATIONID • FS_TRANSACATIONSTATUS **NOTE:** See the Change Auditor User Guide for a description of these email tags and how to configure alert email notifications.

2

Getting Started

- Introduction
- Getting started
- Create File System Auditing template
- Make File System changes and run a report
- Troubleshooting steps

Introduction

Change Auditor for Windows File Servers enables you to search, report and alert on changes to a specific file, folder, or all drives on a Windows file server. You can receive real-time alerts whenever someone tries to access a secure file or folder on a Windows file server.

This section provides a high-level view of the tasks to get you started using Change Auditor for Windows File Servers. It assumes you have successfully installed/licensed Change Auditor for Windows File Servers.

NOTE: Windows File Server auditing is only available if you have licensed Change Auditor for Windows File Servers. 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.**

Getting started

1. Create a new folder on the C: drive of an agented server and then add a new .txt file in this folder. This folder will be used in the following scenarios as an auditing target.
2. To capture events, you must define the files and folders to audit and the operations to capture:
   - Create a File System Auditing template which specifies the files/folders and operations to be audited.
   - Add this template to an agent configuration.
   - Assign the agent configuration to agents.

Create File System Auditing template

For this scenario, we will create a template to audit all changes made to the folder you just created.

1. Select **Start | All Programs | Quest | Change Auditor | Change Auditor Client**.
2. Select **View | Administration**.
3. Click **Auditing**.
4. Select **File System** in the Auditing task list to open the File System Auditing page.
5. Click **Add** to start the File System Auditing wizard which steps you through the process of creating a File System Auditing template.
6. On the first page of the wizard, enter the following information:
   - **Template Name** - Enter a name for the template.
   - **Audit Path** - Select the **Folder** option. Enter the name of the folder previously created (i.e., *Drive:\Folder*\) or click the browse button to select the folder.
   - By default, the scope of coverage for the selected folder will be **This Object and All Child Objects.** Leave this setting for this scenario; however, if you wanted to change this setting, use the drop-down arrow in the scope cell.
   - **Events tab** - Select both the **File Events** and **Folder Events** check boxes (in the header) to track all changes made to the selected folder.
   - **Inclusions tab** - Click on the Inclusions tab, enter * and click **Add** to add it to the Included Names list. Entering * will audit all files and folders in the selected folder.

     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

     NOTE: For file system auditing, the slash characters (\) and double asterisks (**) are not allowed in file masks; therefore to include a specific folder (or share), use the Audit Path field at the top of the page to specify the folder (or share) to audit and enter an * on the Inclusions tab.
   - **Exclusions tab** - Skip the Exclusions tab. (In this scenario, we will not be excluding any subfolders or files from auditing. For more information on using the Exclusions tab, see File System Auditing.)
7. To define any processes that can change audited objects without generating an event, click **Next**.

   On the second page of the wizard, optionally select one or more processes from the list at the top of the page and click **Add** to add them to the list box at the bottom of the page.
8. To create the template and assign it to an agent configuration, expand **Finish** and select **Finish and Assign to Agent Configuration**.
9. On the Configuration Setup dialog select the agent configuration (right pane) to which the template is to be assigned and 'drag and drop' it onto the newly created template**.**

   The **Assigned** cell for the template will change to '**Yes**'.
10. Click **OK** to save your selection, close the dialog and display the Agents Configuration page.
11. If this configuration is not assigned to any agents, you will need to assign it to one or more installed agents at this time.
    - On the Agent Configuration page, select one or more agents from the agent list and click **Assign**.
    - On the Agent Assignment dialog, select the configuration definition to be assigned to the selected agents and click **OK**.

12 On the Agents Configuration page, select the agents assigned to use the modified agent configuration 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.

Make File System changes and run a report

1 To test file system auditing, make some changes to the Windows® file server being monitored.

For example:

- add a .docx or .txt file
- change the security permissions on a file (right-click file, open the Security tab and add another user with full control)
- delete the .txt file
- add a subfolder
- change the security permission of the new folder
- rename the subfolder

2 Select **Start | All Programs | Quest | Change Auditor | Change Auditor Client**) to review the events generated.

3 Open the Searches tab.

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

5 Locate and double-click **All File System Events** in the right pane.

A new Search Results tab is added to the client displaying the Custom File System Monitoring events captured over the last seven days.

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.

Troubleshooting steps

If the Windows file server events do not appear as expected, check the following:

- Verify that the File System Auditing template is assigned to the agent configuration for your agents.
- Refresh the specified agent configurations on the Agent Configuration page to ensure the latest File System Auditing template is being used.
- Verify that you have selected those types of events in the File System Auditing template. (Events tab in the wizard.)
- Verify that you have included the correct subfolders and files in the File System Auditing template. (Inclusions tab in the wizard.)

> **NOTE:** Entering * will include all subfolders and paths.

- Verify that you have not excluded the specified subfolders or files in the File System Auditing template. (Exclusions tab in the wizard.)
- Verify that you have not excluded the process making the file changes in the File System Auditing template. (Last page in the wizard.)

3

File System Auditing

- Introduction
- File System Auditing page
- File System Auditing templates
- File System Auditing wizard
- File System Event settings
- File System event logging

Introduction

To capture Windows file server events, you must define the files/folders to be audited and the events to be captured:

1. Create a File System Auditing template which specifies the files/folders and events to be audited.
2. Add this template to an agent configuration.
3. Assign the agent configuration to agents.

TIP: Quest recommends a phased approach to setting up file/folder auditing for all servers. A phased approach will allow file/folder auditing to be deployed in stages so that the coordinator performance is not degraded.

NOTE: Windows File System auditing is supported in a Windows failover cluster configuration. However, the agent is not aware of the cluster and will only audit the active nodes in the cluster where agents are deployed.

This section provides instructions for creating File System Auditing templates, as well as a description of the File System Auditing page and File System Auditing wizard. 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.

File System Auditing page

The File System Auditing page displays when **File System** is selected from the Auditing task list in the navigation pane of the Administration Tasks tab. From this page you can launch the File System Auditing wizard to specify the file, folder or all drives in a system that are to be audited. You can also edit existing templates, disable a template, 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 *C*hange Auditor User Guide for more information on how to gain access.

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

Template

Displays the name assigned to the template when it was created.

Status

Indicates whether the auditing template is enabled or disabled.

Paths

This field is used for filtering data.

Excluded Processes

This field is used for filtering data.

Click the expansion box to the left of the Template name to expand this view and display the following details for each template:

Path

Displays the name of the file paths or folders included in the File System Auditing template.

Status

Indicates whether auditing for the selected file path is enabled or disabled.

Scope

Indicates the scope of coverage specified for each file path in the selected template:

- This object only
- This object and child objects only
- This object and all child objects

Include

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

Exclude

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.

Excluded Process

Displays a list of the processes excluded from auditing (i.e., changes from these processes are not audited) as specified on the last page of the File System Auditing wizard.

NOTE: The cells directly under the main heading rows are used for filtering data. That is, as you enter characters into these cells, the client will redisplay the templates that meet the search criteria (i.e., comparison operator and characters entered). For more details about using the data filtering function provided throughout the Change Auditor client, see the Change Auditor User Guide.

File System Auditing templates

To enable File System auditing in Change Auditor, you must first create a File System Auditing template which specifies the files, folders, or all drives on a system that are to be audited. This template must then be assigned to the appropriate agents' configuration to audit the specified files and folders.

To create an auditing template for a file:

1. Open the Administration Tasks tab.
2. Click **Auditing**.
3. Select **File System** (under the Server heading in the Auditing task list) to open the File System Auditing page.
4. Click **Add** to open the File System Auditing wizard which will step you through the process of creating a File System Auditing template.
5. On the first page of the wizard, enter the following information:
   - **Template Name** - Enter a name for the template.
   - **Audit Path** - Select the **File** option. Enter a file name (Drive:\Folder\FileName.ext) or click the browse button and select the file to be audited.

     NOTE: This must be a local path. Auditing of network shares or mapped drives is not supported. To audit those files/folders, a Change Auditor agent must be deployed on the share's hosting server.

     Click **Add** to move the specified file to the selection list.
   - **Events tab** - Select the file events to be audited for the file selected in the selection list.

     NOTE: Selecting the **File Events** check box at the top of the events list on the Events tab will select all of the events listed. Similarly, clearing this check box will clear all of the selected events.

   Repeat this step to add additional files to this auditing template.
6. Multiple folder open events are generated by tooltips (folder content information that is displayed when you hover your mouse over a folder) because Windows Explorer navigates the folder tree for all the sub-folders when you hover over the parent folder to see the tooltip. To ignore the folder opened events generated by this action, select the **Discard Windows Explorer tooltip events from folder browsing** option.
7. Multiple file open events are generated by file scans because Windows Explorer opens and reads the header of all files contained in an opened folder for information to display in the window. To ignore the file open events generated by this action, select the **Discard file open events from browsing** option.
8. (Optional) Click **Next** to proceed to the next page to select processes that are to be excluded from auditing (for example, changes made by the processes specified on this page will not be audited).

   Select one or more processes from the process list and click **Add** to move these processes to the exclusion list at the bottom of the page.

   NOTE: You can also view processes on a different server or enter a process not listed in the process list.

9 To create the template without assigning it to an agent configuration, click **Finish**.

This creates the template, closes the wizard, and returns you to the File System Auditing page where the newly created template is now listed.

10 To create the template and assign it to an agent configuration, expand **Finish** and select **Finish and Assign to Agent Configuration**.

On the Configuration Setup dialog, use one of the following methods to assign this template to an agent configuration:

- Select the newly created template and drag and drop it onto a configuration in the Configuration list.
- Select a configuration from the Configuration list and 'drag and drop' it onto the newly created template.
- Select a configuration, then select the newly created template, right-click and select **Assign**.
- Select a configuration, then select the newly created template, click in the corresponding **Assigned** cell and click **Yes**.

11 If this configuration is not assigned to any agents, you will need to assign it to one or more installed agents to capture the specified file system events.

- On the Agent Configuration page, select one or more agents from the agent list and click **Assign**.
- On the Agent Assignment dialog, select the configuration definition to be assigned to the selected agents and click **OK**.
- On the Agent Configuration page, select the agents assigned to use the modified agent configuration 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 create an auditing template for a folder:

1 Open the Administration Tasks tab.

2 Click **Auditing**.

3 Select **File System** (under the Server heading in the Auditing task list) to open the File System Auditing page.

4 Click **Add** to launch the File System Auditing Wizard which steps you through the process of creating a File System Auditing template.

5 On the first page of the wizard, enter the following information:

- **Template Name** - Enter a name for the template.
- **Audit Path** - Select the **Folder** option. Enter a folder name (i.e., *Drive:\Folder*) or click the Browse button to select the folder to audit.

  > **NOTE:** This must be a local path. Auditing and/or protecting network shares is not supported. To audit or protect those files/folders, an agent must be deployed on the share's hosting server.

NOTE: Once the **Folder** option is selected, you can select a system variable using the drop-down menu. Click the arrow to the far right of the text box and select one of the following options:

- Common Program Files
- Program Files
- System Drive
- Windows Directory
- All Shares (Change Auditor does NOT audit any shares that are hidden using the dollar sign character ($) appended to the end of the share name.)

Click **Add** to add the specified folder to the Selection list (middle of the page).

6 By default, the scope of coverage for the selected folder will be **This object and all child objects**. However, you can change the scope, by selecting a different option from the drop-down box in the scope cell of the selection list:

- **This object only**- select this option to audit only the selected folder, not its files or subfolders.
- **This object and child objects only** - select this option to audit the selected folder and its direct files and subfolders. This is not recursive.
- **This object and all child objects** - select this option to audit this folder and all of its files and subfolders.

In addition, selecting the folder entry in the Selection list activates the tabs across the bottom of the page. The settings specified on these tabs apply to the entry selected.

7 On the Events tab, select the file and folder events to be audited.

NOTE: Selecting the **File Events** or **Folder Events** check box at the top of the events list on the Events tab will select all of the events listed. Similarly, clearing these check boxes will clear all of the selected events.

8 On the Inclusions tab, specify the file masks to audit.

NOTE: Do NOT use the Inclusion tab to add additional subfolder paths onto the monitored base path (audit path specified above). It is meant to specify an inclusion mask for ONLY objects located under the monitored base path.

Enter a file mask to specify what is to be included in the 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.

NOTE: For file system auditing, the slash characters (\) and double asterisks (**) are not allowed in file masks; therefore, to include a specific folder (or share), use the Audit Path field at the top of the page to specify the folder (or share) to be audited and enter an * on the Inclusions tab.

For example, entering * will include all subfolders and files in the selected audit path.

You can also enter the name of an individual subfolder or file to be audited. However, if you enter the name of an individual subfolder, you will only receive events for operations performed against that subfolder. You will NOT receive events for operations performed against any child objects under the specified subfolder.

Once you have specified the subfolders/files for inclusion, click **Add** to add it to the Inclusion list at the bottom of the page.

Repeat this step to add additional subfolders and files to the Inclusion list.

9 (Optional) On the Exclusions tab, specify the names and paths of any subfolders or files in the selected audit path that are to be excluded 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.

You can also enter the name of an individual subfolder or file to be excluded from auditing or click the browse button and select one of the options to browse for and select an individual subfolder or file in the specified audit path:

- **Browse Files** - selecting this browse option displays the Select a file system path dialog allowing you to select a file for exclusion from auditing.
- **Browse Folders** - selecting this browse option displays the Browse for Folder dialog allowing you to select a folder for exclusion from auditing.

NOTE: If you select a file or subfolder that does not belong to the selected audit path, the wizard will not allow you to continue. A red flashing icon is displayed indicating that you have selected a file or folder outside of the selected audit path. However, the wizard will not prevent you from entering the name of a file or subfolder that is outside of the audited path. If this happens, Change Auditor will NOT exclude it from auditing.

Once you have specified a subfolder or file for exclusion, use the appropriate **Add** command to add it to the Exclusion list at the bottom of the page:

- **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.

Repeat this step to add additional subfolders and files to the Exclusion list.

10 (Optional) Click **Next** to proceed to the next page to select processes that are to be excluded from auditing (for example, changes made by the processes specified on this page will not be audited).

From this page, select one or more processes from the process list and click **Add** to move these processes to the list at the bottom of the page.

NOTE: You can also view processes on a different server or enter a process not listed in the process list.

11 To create the template without assigning it to an agent configuration, click **Finish**.

This creates the template, closes the wizard, and returns you to the File System Auditing page, where the newly created template is now listed.

12 To create the template and assign it to an agent configuration, expand **Finish** and select **Finish and Assign to Agent Configuration**.

On the Configuration Setup dialog, use one of the following methods to assign this template to an agent configuration:

- Select the newly created template and drag and drop it onto a configuration in the Configuration list.
- Select a configuration from the Configuration list and ‘drag and drop’ it onto the newly created template.
- Select a configuration, then select the newly created template, right-click and select **Assign**.
- Select a configuration, then select the newly created template, click in the corresponding **Assigned** cell and click **Yes**.

13 If this configuration is not assigned to any agents, you will need to assign it to one or more installed agents to capture the specified file system events.

- On the Agent Configuration page, select one or more agents from the agent list and click **Assign**.
- On the Agent Assignment dialog, select the configuration definition to be assigned to the selected agents and click **OK**.
- On the Agent Configuration page, select the agent(s) assigned to use the modified agent configuration 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 modify a template:

1 On the File System Auditing page, select the template to be modified and click **Edit**.

This displays the File System Auditing wizard, where you can modify the files, folders, events and/or processes included in the template.

2 Click **Finish** or expand the **Finish** and select **Finish and Assign to Agent Configuration**.

To disable an auditing template:

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

1 On the File System Auditing page, use one of the following methods to disable a File System 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 disable the auditing of a file path in a template:

1 On the File System Auditing page, use one of the following methods to disable a file path in an auditing template:

- Place your cursor in the **Status** cell for the file path to be disabled, click the arrow control and select **Disabled.**
- Right-click the file path to be disabled and select **Disable.**

The entry in the **Status** column for the selected file path will change to 'Disabled'.

2 To re-enable the auditing of a file path, use the **Enable** option in either the **Status** cell or right-click menu.

To delete an auditing template:

1 On the File System Auditing page, select the template to be deleted and click **Delete | Delete Template**.

2 A dialog displays confirming that you want to delete the selected template. Click **Yes**.

To delete a file path from a template:

1 On the File System Auditing page, select the file path to be deleted and click **Delete | Delete File Path**.

2 A dialog displays confirming that you want to delete the selected file path from the template. Click **Yes**.

NOTE: If the file path is the last one in the template, deleting this file path will also delete the template.

To delete an excluded process from a template:

1. On the File System Auditing page, right-click the excluded process to be deleted from the auditing template and select **Delete**.
2. A dialog will be displayed confirming that you want to delete the selected process from the template. Click **Yes**.

File System Auditing wizard

The File System Auditing wizard displays when you click **Add** or **Edit** on the File System Auditing page. This wizard steps you through the process of creating a new file system auditing template, identifying the files, folders or all drives on a system that are to be included in the auditing template.

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

Create or modify a File System Auditing Template page Use the first page of the wizard to enter a name for the template and specify the individual file or folder or all drives to be audited.	
Template Name	Enter a descriptive name for the template being created.
Audit Path	Select one of the following options to define auditing for a file, folder or all drives: • **File** - select this option to audit a single file. Then enter a file name and path (i.e., *Drive:\Folder\FileName.ext*) or use the browse button to locate and select the file to be audited. • **Folder** - select this option to audit a folder or a set of files. To specify a particular folder, enter the folder's name (for example, *Drive:\Folder*) or use the browse button to select the folder to be audited. Use the drop-down menu to specify a system variable: Common Program Files, Program Files, System Drive, Windows Directory, or All Shares. **NOTE:** This must be a local path. Auditing of network shares or mapped drives is not supported. To audit those files/folders, a Change Auditor agent must be deployed on the share's hosting server. **NOTE:** Change Auditor does NOT audit any shares that are hidden using the dollar sign character ($) appended to the end of the share name. • **All Drives** - select this option to audit all drives. The **Audit Path** text box will contain an asterisk (*) which cannot be changed. Once you have entered the audit path to be audited, use the **Add** button to add it to the selection list.
...	When the **File** or **Folder** option is selected as the audit path, click the browse button to locate and select a file or folder to be audited.
Add	Click **Add** to move the entry in the **Audit Path** text box to the selection list. **NOTE:** Even though you cannot edit the **Audit Path** when the **All Drives** option is selected, you must still use **Add** to move it to the selection list.
Remove	Select an entry in the selection list and click **Remove** to remove it from the template.

Table 2. File System Auditing wizard

Selection list	The list box, located across the middle of this page, displays the files, folders or All Drives selected for auditing. When a Folder is selected, you can use the drop-down menu in the **Scope** field to change the scope of coverage for a folder: • **This object only** - select this option to audit only the selected folder, not its files or subfolders. • **This object and child objects only** - select this option to audit the selected folder and its direct files and subfolders. This is not recursive. • **This object and all child objects** - select this option to audit this folder and all of its files and subfolders. (Default) Select an entry in this list to enable the corresponding Events, Inclusions and Exclusions tabs at the bottom of the page.
Events tab	
Use the Events tab to select the file and/or folder events to audit in the selected audited path. The contents of this tab are based on the entry selected above in the Selection list.	
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. **NOTE:** Due to the potential of generating a very large number of events, **File Open** events are NOT captured when **This object and all child objects** is selected in the Scope cell. Therefore, **File Open** is NOT included in the File Events list on this page when **This object and all child objects** is selected above.
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. **NOTE:** Due to the potential of generating a very large number of events, **Folder Open** events are NOT captured when **This object and all child objects** is selected in the **Scope** cell. Therefore, **Folder Open** is NOT included in the Folder Events list on this page when **This object and all child objects** is selected above.
Ignore specific events	Multiple folder open events are generated by tooltips (folder content information that is displayed when you hover your mouse over a folder) because Windows Explorer navigates the folder tree for all the sub-folders when you hover over the parent folder to see the tooltip. To ignore the folder opened events generated by this action, select the **Discard Windows Explorer tooltip events from browsing** option. Multiple file open events are generated by file scans because Windows Explorer opens and reads the header of all files contained in an opened folder for information to display in the window. To ignore the file open events generated by this action, select the **Discard file open events from folder browsing** option.
Inclusions tab	
When the **Folder** or **All Drives** option is selected in the **Audit Path** field and the **Scope** includes child objects, the Inclusions tab will be displayed allowing you to specify what in the selected audit path is to be audited. **NOTE:** Do NOT use the Inclusion tab to add additional subfolder paths onto the monitored base path (audit path specified above). It is meant to specify an inclusion mask for ONLY objects located under the monitored base path.	

Table 2. File System Auditing wizard

Add the names of subfolders and files to audit	Enter a file mask to specify what in the selected audit path is to be audited. 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. **NOTE:** For file system auditing, the slash characters (\) and double asterisks (**) are not allowed in file masks; therefore to include a specific folder (or share), use the Audit Path field at the top of the page to specify the folder (or share) to be audited and enter an * on the Inclusions tab. 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 to be included. However, if you enter the name of a subfolder, you will only receive events for operations performed against that subfolder. You will NOT receive any events for operations performed against any child objects under the specified subfolder. Once you have specified the subfolder or file to be included, click **Add** to add it to the Inclusions list.
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** - Click 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)	
When the **Folder** or **All Drives** option is selected in the Audit Path field and the Scope includes child objects, the Exclusions tab will be displayed allowing 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 audit path that are to be excluded 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.	

Table 2. File System Auditing wizard

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 to be excluded or use one of the browse options to browse for and select an individual subfolder or file. Click the browse button and select one of the following options: • **Browse Files** - selecting this option displays the Select a file system path dialog allowing you to select an individual file for exclusion. • **Browse Folders** - selecting this option displays the Browse for Folder dialog allowing you to select an individual folder for exclusion. **NOTE:** If you select a file or subfolder that does not belong to the selected audit path, the wizard will not allow you to continue. A red flashing icon is displayed indicating that you have selected a file or folder outside of the selected audit path. However, the wizard will not prevent you from entering the name of a file or subfolder that is outside of the audited path. If this happens, Change Auditor will not exclude it from auditing. Once you have specified a subfolder or file to be excluded, click the appropriate **Add** button to add the file or folder 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 | Folder** - Use this to exclude activity against files/subfolders in any folders that match the exclusion string. • **Add | File** - Select this 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.
(Optional) Select Processes Exempt From Auditing page: Use this page to suppress events generated by a specific process (e.g., anti virus process). **NOTE:** Any file changes performed by the agent service (NpSrvHost.exe process) are excluded from auditing.	
Processes list	Displays a list of the processes available on the local server. From this list, select one or more processes and click **Add** to move them to the Excluded Process list at the bottom of the page.

Table 2. File System Auditing wizard

You are viewing processes on	Displays the name of the server from which the processes list was populated. Click the browse button to select a different server. Selecting this button displays the Select Active Directory Objects dialog. Use the Browse or Search page to locate and select a server. The processes found on that server will then be displayed.
Enter a process not listed above	Select this check box to enter the name of a process that you do not find listed in the Processes list. You can also enter a file mask to select a group of processes 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. • Question mark (?) wildcard character to substitute a single character. Click the **Add** button to add the selected process(es) to the Excluded Process list.
Excluded Process list	The list across the bottom of the page lists the processes that will be allowed to make changes to audited object without generating an event. Use the buttons located above this list box to add and remove processes. • **Add** - Select one or more processes in the Processes list and click **Add** to add the processes to the list. • **Remove** - Select one or more processes in the Excluded Process list and click **Remove** to remove them from the exclusion list.

File System Event settings

From the Agent Configuration page on the Administration Tasks tab you can define how Change Auditor is to handle duplicate file system events.

Use the File System tab at the top of the Configuration Setup dialog to define how to process duplicate file system events.

Discard duplicates that occur within *nn* seconds

This option is selected by default and will discard file system events that occur within 10 seconds of each other. You can enter a value between 1 and 600 (or use the arrow controls) to increase or decrease this interval.

Audit all configured, including duplicates (Not Recommended)

Select this option to audit all configured file system events including duplicate events. This is NOT recommended and therefore is disabled by default.

To set the File System Event settings:

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 **Configurations**.
5. On the Configuration Setup dialog, select an agent configuration from the left-hand pane.
6. Open the File System tab and set the File System Event settings as defined above.

7 Once you have set these settings, click **OK** to save your selections, close the dialog and return to the Agent Configuration page.

8 On the Agent Configuration page, select the agents assigned to the selected agent configuration and click **Refresh 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.

File System event logging

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

For Windows file server events, event logging is disabled by default. When enabled, only configured activities are sent to the Quest File Access event log. See the Change Auditor for Windows File Servers Event Reference Guide for a list of the events that can be sent to this event log.

To enable Windows file server event logging:

1 Open the Administration Tasks tab.

2 Click the **Configuration** task button at the bottom of the navigation pane.

3 Select **Agent** in the Configuration task list to display the Agent Configuration page.

4 Click **Event Logging**.

5 On the Event Logging dialog, select **File System**.

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

The Windows file server events configured in the File System Auditing template will then be sent to the Quest File Access event log.

4

File System Searches/Reports

- Introduction
- Create custom File System search

Introduction

You can search, report and alert on changes to a specific file or folder. Using Change Auditor for Windows File Servers you can receive real-time alerts whenever someone tries to access a secure file or folder.

This section explains how to create a custom file system search using the What tab. For a description of the dialogs mentioned in this chapter, refer to the online help.

Create custom File System search

The following scenario explains how to use the What tab to create a custom File System search.

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:

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** at the top of the Searches page.

   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 options to define the scope of coverage:
   - **All File System Paths** - select to include all file system paths
   - **This Object** - select to include only the selected objects

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

7 By default, **All Actions** is selected meaning that all of the actions associated with the file system path will be included in the search. However, you can clear the **All Actions** option and select individual options to include specific actions in your search definition.

The options available are:

- **All Actions** - select to include all of the actions (Default)
- **Add** - select to include when a File System folder or file is added
- **Delete** - select to include when a File System folder or file is deleted
- **Move** - select to include when a File System folder or file is moved
- **Rename** - select to include when a File System folder or file is renamed
- **Modify** - select to include when a File System folder or file is modified
- **Other** - select to include when any other type of activity occurs on a File System folder or file

8 If you selected a scope other than **All File System Paths**, select the type of file system paths to be included in the search:

- **All Types** - select to search all of the file system path types listed
- **File** - select to search only files
- **Folder** - select to search only folders
- **Transaction** - select to audit changes that were committed or rolled back within a transaction

> **NOTE:** If the **All Types** check box is selected by default, you must clear this check box before you can select any of the other options.

9 If you selected a scope other than **All File System Paths**, enter or use the browse button to select the file or folder to be searched. Once you have entered a file or folder in the **Path** field, click **Add** to add the file/folder to the File System list.

> **NOTE:** Select the **Exclude the Above Selection(s)** check box if you want to search for all file system files or folders EXCEPT those listed in the 'what' list.

> **NOTE:** Select the **Runtime Prompt** check box on this dialog to prompt for a file system path every time the search is run.

10 Once you have selected the file system paths to be included in the search, click **OK** to save your selection and close the dialog.

11 Once you have defined the search criteria, you can either save the search definition or run the search.

- To save the search definition without running it, click **Save**.
- To save and run the search, click **Run**.

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

5

File System Protection

- Introduction
- File System Protection page
- File System Protection templates
- File System Protection wizard

Introduction

When licensed, Change Auditor for Windows File Servers also provides an access control model that permits administrators to secure business-critical files and folders on the file server against potentially dangerous changes.

NOTE: File System protection is designed to provide protection coverage for a small number of business-critical files/folders. Protecting an entire drive or a large portion of a drive is not recommended and has the potential of causing performance impacts and poor user experience.

To use file system protection, you must first define the files/folders to protect:

1. Create a File System Protection template which specifies the files/folders to be protected.
2. Add this template to an agent configuration.
3. Assign the agent configuration to Change Auditor agents.

This section provides instructions for creating File System Protection templates, as well as a description of the File System Protection page and File System Protection wizard. For a description of the dialogs mentioned in this chapter, refer to the online help.

File System Protection page

The File System Protection page displays when **File System** is selected from the Protection task list in the navigation pane of the Administration Tasks tab. From this page you can launch the File System Protection wizard to specify a file or folder to be protected from unauthorized access. You can also edit existing templates, disable a template, 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 File System Protection page contains an expandable view of all the File System Protection templates that have been previously defined. To add a new template to this list, click **Add**. Once added, the following information is provided for each template:

Template

Displays the name assigned to the template when it was created.

Status

Indicates whether the template is enabled or disabled. To enable/disable the template, place your cursor in this **Status** cell, click the arrow control and select the appropriate option from the drop-down menu.

Override Accounts

Indicates whether the override accounts listed are excluded from protection or included in protection. This setting corresponds to the option used at the top of the last page of the File System Protection wizard:

- Excluded from Protection - indicates you selected the **Allow** option to allow only the selected accounts to change the protected objects.
- Included in Protection - indicates you selected the **Deny** option to allow all accounts to change the protected objects EXCEPT for those selected.

Paths

This field is used for filtering data.

Override Account Filter

This field is used for filtering data.

Click the expansion box to the left of the Template name to expand this view and display the following details for each template:

Path

Displays the name of the file system included in the File System Protection template.

Status

Indicates whether the protection for the file path is enabled or disabled.

Subfolders

Indicates whether subfolders under the file system path are also being protected.

Protect

Indicates whether a file system path is to be protected (Yes) or excluded from protection (No).

File Masks

Displays the file masks specified on the first page of the wizard.

Applies To

Indicates what is being protected: Files and Folders, Files, Folders, or Shares.

Protection Type

Indicates the type of operation(s) to be prevented as specified on the first page of the wizard.

Override Account

Displays any accounts that are allowed (or not allowed) to change the protected files/folders, as specified on the last page of the wizard.

NOTE: This field is not displayed when there are no override accounts specified in the File System Protection wizard.

NOTE: The cells directly under the main heading rows are used for filtering data. That is, as you enter characters into these cells, the client will redisplay the templates that meet the search criteria (i.e., comparison operator and characters entered). For more details about using the data filtering function provided throughout the client, see the Change Auditor User Guide.

File System Protection templates

To enable protection, create a File System Protection template which specifies the files/folders to lock down. You can then add this template to an agent configuration, which then needs to be assigned to the appropriate agents.

NOTE: If you are planning to use multiple File System Protection templates, refer to the Change Auditor Technical Insight Guide for more information on how multiple protection templates are evaluated.

NOTE: You can also open the protection wizard from the event details pane. Simply open the Search Results tab, select an event, and click the Protect Object button.

To create a protection template:

1. Open the Administration Tasks tab.
2. Click **Protection**.
3. Select **File System** under the Protection task list to open the File System Protection page.
4. Click **Add** to open the File System Protection wizard which steps you through the process of creating a File System Protection template.
5. In the **Template Name** field, enter a descriptive name for the template.
6. In the **Path** field, enter or click the Browse button to specify the file system path to protect. Click **Add** to move the specified file system path to the selection list.

   NOTE: This must be a local path. Auditing and/or protecting network shares is not supported. To audit or protect those files/folders, an agent must be deployed on the share's hosting server.

7. By default, protection includes the subfolders in the selected file system path. However, to exclude the subfolders, click the arrow control in the **Subfolders** cell and select **No**.
8. By default, the specified system file path will be protected. However, to exclude the selected file system path from protection, click the arrow control in the **Protect** cell and select **No**.
9. By default, protection will be applied to both files and folders in the selected file system path. To protect just files, folders or shares, click the arrow control in the **Applies To** cell and select one of the following options:
   - **Files**
   - **Folders**
   - **Files and Folders** (default)
   - **Shares**
10. By default, protection will prevent ‘all’ operations from occurring. However, to protect against specific operations, click the arrow control in the **Protection Type** cell and select one or more of the following operations:
    - **[All]** (default)
    - **Read**
    - **Write**
    - **Create**
    - **Delete**

- **Rename**
- **Move**
- **Dacl Change**
- **Owner Change**
- **Sacl Change**
- **Attribute Change**
- **CAP Change**
- **Classification Change**

11 Use the **File Mask** field to optionally specify a file mask to protect a group of files in the selected file system path. Once you have specified a file mask, click **Add** to add it to the list at the bottom of the page.

12 On the next page of the wizard, use the Browse or Search page to optionally select user or group accounts which will be allowed to make changes to the protected objects selected on the previous page. Click **Add** to add the selected user or group to the Override Account list.

> **NOTE:** The **Allow** option is selected by default indicating that the selected users or groups will be allowed to change the protected objects. However, you can select the **Deny** option at the top of this page and select individual users or groups that are NOT allowed to change the protected objects. When using the **Deny** option, you are allowing all users and groups to change the protected objects except for those selected on this page.

13 On the next page of the wizard, you have the option to schedule when the protection will be enforced. You can either select to have the protection always run or have it run only during specific times. To enable the protection only during specific times, select the **Protection is scheduled** option, and define when it should be enabled (hour blocks on a weekly basis). The times selected are the local agent time where the template is applied.

> **NOTE:** If you have denied specific users or groups the ability to change the protected objects and you have enabled a protection schedule, those users or groups will be denied access ONLY during this time. Anytime outside of when the schedule is set to enabled, these denied accounts WILL be able to access the protected object.
>
> When the schedule is disabled, ALL options are disabled with it, including any denied access to the specified users. The scheduling options override all other protection settings.

14 On the next page of the wizard, you have the option to control when the protection is enabled based on the location. Location refers to the computer that is attempting to access the resource that is protected.

- **Protect access from all locations**: Protection is always enabled regardless of the location.
- **Protect access only from select locations**: Protection is only enabled for the specified locations.
- **Disable protection only for select locations**: Protection is disabled for the selected locations. Enabled everywhere else.
- **Protect access from all unknown locations**: All file system requests from locations that cannot be determined by the agent will be protected.

> **NOTE:** If you have denied specific users or groups access to protected objects, but you have specified locations that CAN access the protected object, the denied user or group WILL be able to access the protected objects from these locations.
>
> The location options override all other protection settings.

15 To create the template without assigning it to an agent configuration, click **Finish**.

Clicking **Finish** creates the template, closes the wizard, and returns you to the File System Protection page where the newly created template is now listed.

16 To create the template and assign it to an agent configuration, expand **Finish** and select **Finish and Assign to Agent Configuration**.

On the Configuration Setup dialog, use one of the following methods to assign this template to an agent configuration:

- Select the newly created template and 'drag and drop' it onto a configuration in the Configuration list.
- Select a configuration from the Configuration list and 'drag and drop' it onto the newly created template.
- Select a configuration, then select the newly created template, right-click and select **Assign**.
- Select a configuration, then select the newly created template, click in the corresponding **Assigned** cell and click **Yes**.

17 If this configuration is not assigned to any agents, you will need to assign it to one or more installed agents to capture the specified file system events.

- On the Agent Configuration page, select one or more agents from the agent list and click the **Assign** tool bar button.
- On the Agent Assignment dialog, select the configuration definition to be assigned to the selected agents and click **OK**.
- On the Agent Configuration page, select the agents assigned to use the modified agent configuration 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 modify a template:

1 On the File System Protection page, select the template to be modified and click **Edit**.

This displays the File System Protection wizard, where you can modify the files or folders to be protected.

2 Click **Finish** or expand **Finish** and select **Finish and Assign to Agent Configuration**.

To disable a template:

The disable feature allows you to temporarily stop protecting the specified file path without having to remove the protection template or individual file path from an active template.

1 On the File System Protection page, use one of the following methods to disable a 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 protection template, use the **Enable** option in either the **Status** cell or right-click menu.

To disable the protection of a file path in a template:

1 On the File System Protection page, use one of the following methods to disable a file path in a protection template:

- Place your cursor in the **Status** cell for the file path to be disabled, click the arrow control and select **Disabled**.
- Right-click the file path to be disabled and select **Disable**.

The entry in the **Status** column for the selected file path will change to 'Disabled'.

2 To re-enable protection of a file path, use the **Enable** option in either the **Status** cell or right-click menu.

To delete a template:

1. On the File System Protection page, select the template to delete and click **Delete | Delete Template**.
2. A dialog displays confirming that you want to delete the selected template. Click **Yes**.

To delete a file path from a template:

1. On the File System Protection page, select the file path to be deleted and click **Delete | Delete File Path**.
2. A dialog displays confirming that you want to delete the selected file path from the template. Click **Yes**.

NOTE: If the file path is the last one in the template, deleting this file path will also delete the template.

File System Protection wizard

The File System Protection wizard displays when you click **Add** or **Edit** on the File System Protection page. This wizard steps you through the process of creating a new file system protection template, identifying the files and/or folders to be included in the template.

NOTE: You can also open the protection wizard from the event details pane. Simply open the Search Results tab, select an event, and click the Protect Object button.

The following table provides a description of the fields and controls in the File System Protection 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.

Table 3. File System Protection wizard

Create or modify a File System Protection Template page	
Use the first page of the wizard to enter a name for the template and specify the file system path to be protected.	
Template Name	Enter a descriptive name for the template being created.
Path	Enter or use the browse button to specify the file system path to be protected. After entering or selecting the files system path to be protected, click the **Add** button to add it to the File System Path list. **NOTE:** This must be a local path. Auditing and/or protecting network shares is not supported. To audit or protect those files/folders, an agent must be deployed on the share's hosting server.
...	Selecting the browse button displays the Browse For Folder dialog allowing you to browse for and select the file system path which is to be protected by Change Auditor.
File System Path list	The file system paths selected for protection are displayed in the list box located in the middle of the page. Use the buttons to the right of the **Path** field to add and remove file system paths. • **Add** - Click to move the entry in the **Path** text box to the File System Path list. • **Remove** - Select an entry in the File System Path list and click **Remove** to remove it.
Subfolders	By default, protection will include the subfolders in the selected file system path. However, if you want to exclude subfolders from protection, click the arrow control in the **Subfolders** cell and click **No**.
Protect	By default, the specified file system path will be protected. However, to exclude the selected file system path from protection, click the arrow control in the **Protect** cell and click **No.**

Table 3. File System Protection wizard

Applies To	By default, protection will be applied to both files and folders in the selected file system path. To protect just files, folders or shares, click the arrow control in the **Applies To** cell and select one of the following options: • **Files** • **Folders** • **Files and Folders** (default) • **Shares**
File Mask	If applicable, this cell displays the file mask, which is used to protect a group of files, as specified at the bottom of the page.
Protection Type	By default, protection will prevent 'all' operations from occurring. However, to protect against specific operations, click the arrow control in the **Protection Type** cell and select one or more of the following operations: • **[All]** (default) • **Read** • **Write** • **Create** • **Delete** • **Rename** • **Move** • **Dacl Change** • **Owner Change** • **Sacl Change** • **Attribute Change** • **CAP Change** • **Classification Change** **NOTE:** File classifications are modified by a system process on behalf of a user; therefore, a system/machine account may not be captured for the 'who' for file classification changes. As a result, classification operations specified in a File System Protection template may not be affected by the 'Allow/Deny' accounts specified on the next page of the protection wizard.
File Mask	Use this field to optionally specify a file mask to protect a group of files. You can use any combination of ? or * wildcard characters. Once you have specified a file mask, click **Add** to add it to the list at the bottom of the page and the **File Masks** cell in the File System Path list (middle of the page).
File Masks list	The list box at the bottom of the page lists the file masks specified for this protection template. Use the buttons to the right of the **File Mask** field to add and remove masks. • **Add** - Click to move the entry in the text box to the File Masks list. • **Remove** - Select an entry in the File Masks list and click **Remove** to remove it
(Optional) Select Accounts Allowed (Not allowed) to Access Protected Objects page	
Use this page to optionally specify user and group accounts that are authorized to make changes to the specified protected objects.	
Allow	The **Allow** option is selected by default indicating that the accounts selected on this page will be the only accounts allowed to make changes to the protected objects. Use the Browse or Search page to select the user or group accounts.

Table 3. File System Protection wizard

Deny	Select the **Deny** option if you would like to allow all users and groups to change the protected objects EXCEPT for those selected on this page. Use the Browse or Search page to select the user or group accounts.
Browse page	Displays a hierarchical view of the containers in your environment allowing you to locate and select the users or groups that will be allowed (not allowed) to change the protected objects. Once you have selected an account, use **Add** to add it to the list at the bottom of the page.
Search page	Use the controls at the top of the Search page to search your environment to locate the users or groups that will be allowed (not allowed) to change the protected objects. Once you have selected an account, use **Add** to add it to the list at the bottom of the page.
Options page	Use the Options page to modify the search options used to retrieve directory objects.
NOTE: For more information on using the Browse, Search or Options pages, please refer to Directory Object Picker in the online help or Change Auditor User Guide.	
Override Account list	The list box across the bottom of the page displays the user and group accounts that are allowed (not allowed) to change the protected objects selected on the previous page of the wizard. Use the buttons located above this list box to add and remove accounts. • **Add** - Select an account in the Browse or Search page and click **Add** to add it to the Override Account list. • **Remove** - Select an account in the Override Account list and click **Remove** to remove it.

Table 3. File System Protection wizard

(Optional) Schedule when protection is enabled	You can either select to have the protection always run or have it run only during specific times. To enable the protection only during specific times, select the Protection is scheduled option, and define when it should be enabled (hour blocks on a weekly basis).The times selected are the local agent time where the template is applied. **NOTE:** If you have denied specific users or groups the ability to change the protected objects and you have enabled a protection schedule, those users or groups will be denied access ONLY during this time. Anytime outside of when the schedule is set to enabled, these denied accounts WILL be able to access the protected object. When the schedule is disabled, ALL options are disabled with it, including any denied access to the specified users. The scheduling options override all other protection settings.
(Optional) Enable or disable protection for specific location	Control when the protection is enabled based on the location. Location refers to the computer that is attempting to access the resource that is protected. Select from the following options: • Protect access from all locations: Protection is always enabled regardless of the location. • Protect access only from select locations: Protection is only enabled for the locations specified in the list box. • Allow access only from select locations: Protection is disabled for the select locations. Enabled everywhere else. • Protect access from all unknown locations: All file system requests from locations that cannot be determined by the agent will be protected. **NOTE:** If you have denied specific users or groups access to protected objects, but you have specified locations that CAN access the protected object, the denied user or group WILL be able to access the protected objects from these locations. The location options override all other protection settings.

6

File System Events

The following events can be selected for auditing from the Events tab on the File System Auditing wizard. The events listed on the Events tab is based on the file/folder specified in the **Audit Path** and the coverage specified in the **Scope** cell.

File Events

- Failed file access (NTFS permissions)
- Failed file access (Change Auditor Protection)
- File access rights changed
- File attribute changed
- File auditing changed
- File central access policy changed
- File classification changed
- File created
- File deleted
- File last write changed
- File moved
- File opened

  NOTE: This event is not available when **This object and all child objects** is selected in the **Scope** cell.

- File ownership changed
- File renamed

Folder Events

- Failed folder access (NTFS permissions)
- Failed folder access (Change Auditor Protection)
- Failed share access (NTFS permissions)

  NOTE: The Failed share access (NTFS) event monitors changes made to a share's properties (such as share permissions and comments). It does NOT monitor failed access to a share from a remote computer. So if a user tries to read or change a share's property, the event will be triggered.

  The Failed share access (Change Auditor Protection) event works similarly. Once you have the share protected, only attempts to change a share's property will generate the 'failed share access' event; not attempts to access the share itself.

- Failed share access (Change Auditor Protection)
- Folder access rights changed
- Folder attribute changed

- Folder auditing changed
- Folder central access policy changed
- Folder classification changed
- Folder created
- Folder deleted
- Folder moved
- Folder opened

  NOTE: This event is not available when **This object and all child objects** is selected in the **Scope** cell.

- Folder ownership changed
- Folder renamed
- Junction point created
- Junction point deleted
- Local share added
- Local share folder path changed
- Local share permissions changed
- Local share removed

NOTE: The following File System events are not listed on the Events page of the File System Auditing wizard because they are always captured when you have applied a Change Auditor for Windows File Servers license:

- Shadow Copy created
- Shadow Copy deleted
- Shadow Copy rolled back
- Transaction Status changed

7

File/Folder Inclusion and Exclusion Examples

This appendix 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.

The Inclusions and Exclusions tabs only appear when the **Folder** or **All Drives** option is selected in the **Audit Path** field and the **Scope** includes child objects. 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.

NOTE: For file system auditing, the slash characters (\) and double asterisks (**) are not allowed in file masks; therefore, to include a specific folder (or share), use the Audit Path field at the top of the page to specify the folder (or share) to be audited and enter an * on the Inclusions tab.

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 4. Inclusion examples

What to include in 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 4. Inclusion examples

What to include in 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 = Folder (<Drive>:\<FolderName>\)

NOTE: When the Auditing Path is **All Shares**, you cannot specify to exclude an individual share or folders/files found on an individual shares; you can only specify to exclude files and/or folders which may be found on all shares. Change Auditor automatically appends *\ to the beginning of all exclusion entries when the Audit Path is **All Shares.**

In the following examples the Audit Path is C:\TEMP\.

Table 5. Exclusion examples: Audit Path = Folder

What to exclude:	Exclusion syntax/examples:
Exclude activity against files/subfolders in the specified folder in the base audit path. (**Add | Folder**)	**Exclusion Syntax:** <*FolderName*> **Example:** DOCS **Excludes:** C:\TEMP\DOCS
Exclude activity against files/subfolders in all folders with a specific name, which may be found anywhere in the audit path. (**Add | Folder**)	**Exclusion Syntax:** **\<*FolderName*> **Example:** **\MYDOCS **Excludes:** C:\TEMP\MYDOCS C:\TEMP\DOCUMENTS\MYDOCS C:\TEMP\DOCS\PRIVATE\MYDOCS

Table 5. Exclusion examples: Audit Path = Folder

What to exclude:	Exclusion syntax/examples:
Exclude activity against files/subfolders in all folders that contain a specific string in their name. (**Add | Folder**)	**Exclusion Syntax:** <*FolderNameString*> **Example 1:** DOC* **Excludes:** Folders whose name begins with 'DOC' which are located in the base audit path. HOME\TEMP\DOCS HOME\TEMP\DOCUMENTS **Example 2:** **DOC **Excludes:** Folders whose name ends in 'DOC' which may be located anywhere in the audit path. C:\TEMP\MYDOC C:\TEMP\DOCS\PRIVATE\DOC **Example 3:** **DOC* **Excludes:** Folders whose name contains 'DOC' which may be located anywhere in the audit path. C:\TEMP\DOCS C:\TEMP\DOCUMENTS C:\TEMP\MYDOCS C:\TEMP\FINALDOC C:\TEMP\PUBLIC\DOCS C:\TEMP\TEST\BETA\DOCUMENTS
Exclude activity against files whose name contains a specific character string, which may be found anywhere in the audit path. (**Add | File**)	**Exclusion Syntax:** **<*CharString*>* **Example:** **DOC* **Excludes:** C:\TEMP\Test1.docx C:\TEMP\Doc1.tmp C:\TEMP\TEST\BETA\FinalDocument.pdf
Exclude activity against a specific file in the base audit path. (**Add | File**)	**Exclusion Syntax:** <*FileName.Ext*> **Example:** Test1.docx **Excludes:** C:\TEMP\Test1.docx
Exclude activity against all files with a specific extension, which are located in the base audit path. (**Add | File**)	**Exclusion Syntax:** *.<*Ext*> **Example:** *.tmp **Excludes:** C:\TEMP\Doc1.tmp C:\TEMP\Testing123.tmp

Table 5. Exclusion examples: Audit Path = Folder

What to exclude:	Exclusion syntax/examples:
Exclude activity against all files with a specific extension, which may be found anywhere in audit path. (**Add | File**)	**Exclusion Syntax:** **.<*Ext*> **Example:** **.tmp **Excludes:** C:\TEMP\Doc1.tmp C:\TEMP\DOCUMENTS\Testing.tmp C:\TEMP\TEST\BETA\Draft1.tmp
Exclude activity against all files that contain a specific string in their name and/or file extension, which are located in the base audit path. (**Add | File**)	**Exclusion Syntax:** <*FileNameString*>.<*ExtString*> **Example 1:** ??word.??? **Excludes:** Files whose name contains six characters and ends in 'word', with a three character file extension, found in the base audit path. C:\TEMP\Myword.doc C:\TEMP\12word.txt **Example 2:** *word*.??p **Excludes:** Files whose name contains the string 'word', with a three character file extension that ends with the letter 'p'. C:\TEMP\Word.tmp C:\TEMP\Mywordtest.tmp C:\TEMP\Nowords.bmp

Audit Path = All Drives

In the following examples, there are two drives: C and D.

NOTE: When the Auditing Path is **All Drives**, you cannot specify to exclude an individual drive or folders/files found on an individual drive; you can only specify to exclude files and/or folders which may be found on all drives. Change Auditor automatically appends *\ to the beginning of all exclusion entries when the Audit Path is **All Drives**.

Table 6. Exclusion examples: Audit Path = All Drives

What's to be excluded:	Exclusion syntax/examples:
Exclude activity against files/subfolders in a specific folder and path that may be found anywhere on all drives. (**Add | Folder**) **NOTE:** You cannot specify an absolute path when the Audit Path is **All Drives**.	**Exclusion Syntax:** ****<*Path*>\<*FolderName*> **Example:** **USERS\TEMP\DOCS **Excludes:** C:\USERS\TEMP\DOCS D:\USERS\TEMP\DOCS D:\SHARED\APPS\USERS\TEMP\DOCS
Exclude activity against files/subfolders in all folders with the specified folder name, which may be found anywhere on all drives. (**Add | Folder**)	**Exclusion Syntax:** **\<*FolderName*> **Example:** **\DOCS **Excludes:** C:\USERS\TEMP\DOCS C:\DOCUMENTS\CHANGEAUDITOR\TEST\DOCS D:\USERS\TEMP\DOCS D:\SHARED\APPS\USERS\TEMP\DOCS

Table 6. Exclusion examples: Audit Path = All Drives

What's to be excluded:	Exclusion syntax/examples:
Exclude activity against files/subfolders in all folders whose name ends in a specified string, which is located in the base audit path. **NOTE:** The base audit path refers to the top level drive letter when **All Drives** is specified. **(Add | Folder)**	**Exclusion Syntax:** **<FolderNameString>* **Example:** *DOC **Excludes:** C:\DOC C:\TESTDOC D:\DOC
Exclude activity against files/subfolders in all folders whose name contains a specific string of characters, which may be found anywhere on all drives. (**Add | Folder**)	**Exclusion Syntax:** **<CharString>** **Example:** **DOC* **Excludes:** C:\DOCUMENTS C:\MYDOCS C:\USERS\TEMP\DOCS D:\USERS\TEMP\DOCS D:\SHARED\APPS\INSTALLDOC D:\SHARED\APPS\USERS\TEMP\DOCS
Exclude activity against files whose name contains a specific string of characters, which may be found anywhere on all drives. (**Add | File**)	**Exclusion Syntax:** **<CharString>** **Example:** **DOC* **Excludes:** C:\TEMP\Test1.docx C:\TEMP\Doc1.tmp C:\USERS\TEMP\DOCS\Test1.doc C:\TEMP\TEST\BETA\FinalDocument.pdf D:\SHARED\APPS\USERS\TEMP\OldDocPlan
Exclude activity against files whose name ends with a specific string (regardless of the extension), that may be found anywhere on all drives. (**Add | File**)	**Exclusion Syntax:** ***<FileName>.** **Entering:** **test1.** **Excludes:** C:\TEMP\Test1.docx C:\DEPTS\TECHNICALDOCS\MyTest1.doc C:\USERS\DOCS\NewTest1.docx D:\SHARED\APPS\USERS\TEMP\Test1.xlsx
Exclude a file with a specific file name (regardless of the extension), that is found at the second level of a path on all drives. (**Add | File**)	**Exclusion Syntax:** **\<FileName>.** **Entering:** *\test1.** **Excludes:** C:\TEMP\Test1.docx D:\SHARED\Tests1.xls
Exclude activity against all files with a specific extension, which are located in the base audit path. **NOTE:** The base audit path refers to only the top level drive letter when **All Drives** is specified. (**Add | File**)	**Exclusion Syntax:** *.*<Ext>* **Example:** *.tmp **Excludes:** C:\Doc1.tmp C:\Testing123.tmp D:\MyTest.tmp
Exclude activity against all files with the specified file extension found anywhere on all drives. (**Add | File**)	**Exclusion Syntax:** **.*<Ext>* **Example:** **.pdf **Excludes:** C:\DOCUMENTS\Test123.pdf C:\TEST\DOCS\Current.pdf C:\TEMP\TEST\BETA\FinalDocument.pdf D:\ReleaseHistory.pdf D:\SHARED\APPS\WhatsNew.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 Microsoft 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.