Quest

Quest® Change Auditor for NetApp® 7.1

User Guide

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

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

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

Patents

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

Trademarks

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

Legend

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

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

Change Auditor for NetApp User Guide
Updated - June 2020
Software Version - 7.1

Contents

Change Auditor for NetApp Overview 5
Introduction 5
System overview 6
Deployment requirements 7
FPolicy limitation 7
Client components and features 7

Getting Started 9
Introduction 9
Verify auditing template is applied 9
Make changes and run a report 9
Troubleshooting steps 10

NetApp Filer Auditing 12
Introduction 12
NetApp Auditing page 12
NetApp Auditing templates 13
NetApp Auditing wizard 19
File System events settings 22
NetApp event logging 23

NetApp Searches/Reports 24
Introduction 24
Create custom NetApp searches 24

Performance Considerations 27
Change Auditor agent performance 27
Hardware considerations 27
Load balancing 27
Configuring audit scope 28

NetApp Filer Events 29

File and Folder Inclusion and Exclusion Examples 30
Inclusions tab 30
Exclusions tab 32
Folder exclusion examples 32
Volume exclusion examples 34
All volume exclusion examples 37

About us 39
We are more than just a name 39
Our brand, our vision. Together. 39
Contacting Quest 39

Technical support resources 39

1

Change Auditor for NetApp Overview

- Introduction
- System overview
- Deployment requirements
- FPolicy limitation
- Client components and features

Introduction

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

Change Auditor for NetApp captures audited events and provides detailed information about the following filer activity:

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

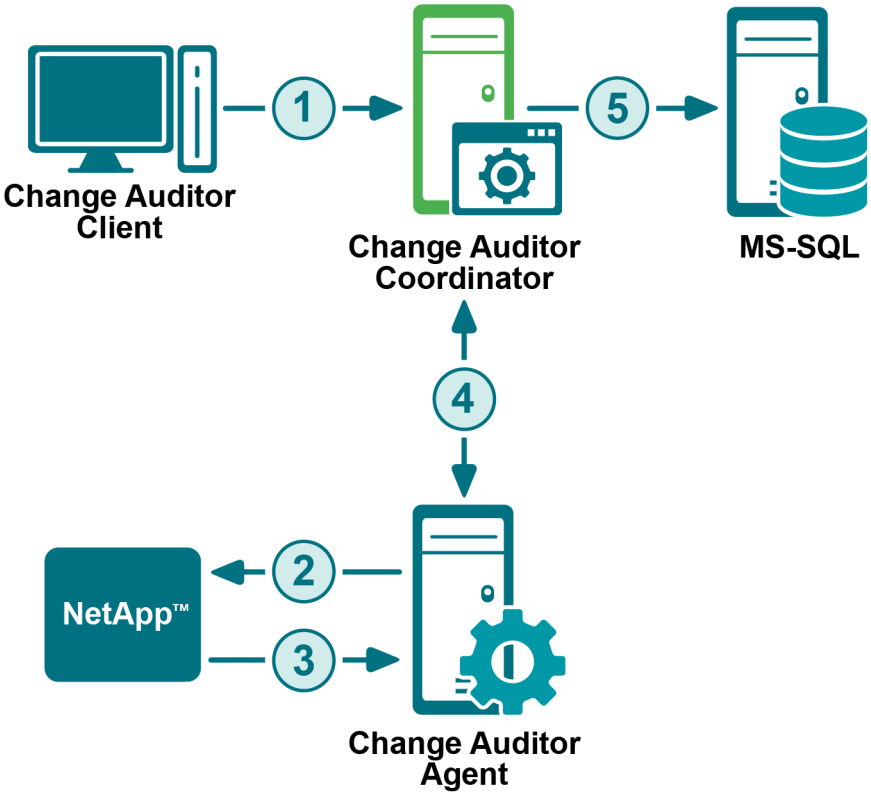
Change Auditor for NetApp functionality is based on the NetApp Data ONTAP file screening policy (FPolicy). This policy allows third-party file screening software to interact with the NetApp filer.

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

System overview

The following diagram illustrates how NetApp integrates with Change Auditor to provide this auditing capability.



1 Using the Change Auditor client, users create a NetApp auditing template to specify the NetApp filer location and select the agent to receive the NetApp events.

2 The specified agent registers with the FPolicy screening policy to capture the NetApp events based on the auditing scope defined in the NetApp auditing template.

3 The NetApp filer forwards detailed information about the changes and activities back to the agent.

4 The agent processes the NetApp events and forwards them on to the coordinator. The coordinator is responsible for fulfilling client and agent requests.

5 The coordinator then forwards the events and related details to the Change Auditor database.

Deployment requirements

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

NOTE: This guide assumes NetApp ONTAP is properly installed and configured. For detailed installation steps, see the appropriate guides from NetApp.

To audit NetApp, you need to:

- Verify that Common Internet File System (CIFS) is setup for NTFS files only.
- Verify that CIFS is enabled and running.
- Define a separate NetApp Auditing template for each NetApp filer to audit.

FPolicy limitation

File changes to a NetApp filer initiated from the server hosting the agent responsible for capturing NetApp events will not be reported by the filer. This is a limitation of the NetApp filer's FPolicy and not a limitation of Change Auditor.

Client components and features

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

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

Table 1. Change Auditor for NetApp client components/features

Client page	Feature
Administration Tasks tab	Agent Configuration page • Event Logging - enable/disable NetApp 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 • NetApp **NOTE:** See NetApp Filer Auditing for information on enabling event logging, viewing/modifying the agent configuration settings, and creating templates to define NetApp auditing.
Event Details pane	What details • Path • Process
Events	Facilities • NetApp

Table 1. Change Auditor for NetApp client components/features

Client page	Feature
Searches page	Built-in reports • Reports that include NetApp events.

2

Getting Started

- Introduction
- Verify auditing template is applied
- Make changes and run a report
- Troubleshooting steps

Introduction

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

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

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

Verify auditing template is applied

To ensure NetApp events are being captured, check to see if the agent assigned to the NetApp Auditing template is using the latest agent configuration.

To verify that latest agent configuration is being used:

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

Make changes and run a report

1. To test NetApp filer auditing, make some changes to the NetApp filer being monitored.

   For example:

   - create a new folder
   - rename the folder

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

2 Select **Start | All Programs | Quest | Change Auditor | Change Auditor Client** 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 NetApp Events** in the right pane.

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

6 Double-click an event from the Search Results grid to display the event details for the selected event.

Troubleshooting steps

If the NetApp events do not appear as expected, check the following:

- Verify that the NetApp filer is valid for the NetApp Auditing template. The **NetApp Filer** field should contain the NetBIOS name or IP address of the NetApp filer to be audited. The wizard does not validate this entry when it is entered.
- Verify that the agents assigned to the NetApp auditing template are not on the servers that are initiating file changes to the NetApp filer. (This is a limitation with the NetApp filer's FPolicy.)
- Verify that the following options have been configured on the servers hosting the agents assigned to a NetApp Auditing template:
  - Reverse DNS zone must be configured and functional in your domain.
  - If Windows Firewall is enabled, it must be configured to allow 'File Sharing'.

  See the Release Notes for required rights and permission.
- Verify that all of the agents assigned to a NetApp Auditing template have their user account in the local Administrators group of the NetApp filer or that you have specified the NetApp filer credentials in the NetApp Auditing wizard. See the Release Notes for required rights and permission.
- Verify that you have selected those types of events in the NetApp Auditing template. (Events tab in the wizard.)
- Verify that you have included the correct subfolders and paths in the NetApp 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 paths in the NetApp Auditing template. (Exclusions tab in the wizard.)
- Refresh the specified agent configurations on the Agent Configuration page to ensure the latest NetApp Auditing template is being used.
- Verify what version of Data ONTAP is being used. That is, NetApp filers running version 7.2 (or earlier) will NOT capture the File/Folder Ownership Changed or File/Folder Access Rights Changed events.

- If you are using an older version of Data ONTAP, you may need to upgrade to version 7.3.4 (or later) in order to capture events.

3

NetApp Filer Auditing

- Introduction
- NetApp Auditing page
- NetApp Auditing templates
- NetApp Auditing wizard
- File System events settings
- NetApp event logging

Introduction

You must define a separate NetApp auditing template for each NetApp filer to be audited by Change Auditor. The NetApp Auditing page on the Administration Tasks tab displays details about each NetApp Auditing template created and allows you to add new auditing templates.

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

NetApp Auditing page

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

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

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

Filer

Displays the name of the NetApp filer specified in the wizard.

Status

Indicates whether the auditing template is enabled or disabled.

Paths

This field is used for filtering data.

Click the expansion box to the left of the Filer name to expand this view and display the following details:

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.

Path

Displays the name of the audit paths included in the NetApp Auditing template.

Status

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

Include Mask

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

Scope

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

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

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.

Agent

Lists the Change Auditor agents assigned to monitor the selected NetApp filer.

User

Displays the name of the user account that has access to the NetApp filer. This information is only displayed when **Set Credentials** is used on the second page of the wizard to specify the NetApp filer credentials to be used by a Change Auditor agent.

NetApp Auditing templates

To enable NetApp filer auditing, create a NetApp Auditing template for each NetApp filer to audit. Each auditing template defines the NetApp filer to be audited, the auditing scope, and the agents that are to receive the NetApp events.

NOTE: There can be only one NetApp Auditing template per NetApp filer. Therefore, if you want to audit multiple audit paths, use the same template to specify all the audit paths to be audited on the selected NetApp filer.

NOTE: For NetApp 7-mode, you must enable TLS communication on the filer to allow secure communication with the Change Auditor client using the following command: `options tls.enable on`

To audit a file:

1. Open the NetApp Auditing wizard (Click **Add** or **Edit** on NetApp Auditing page).
2. On the first page of the wizard, enter the following information:
   - **NetApp Filer** - Select the NetApp filer from the drop-down or enter the NetBIOS name or IP address of the NetApp filer to be audited.
   - File and folder auditing is supported in both 7-mode (non-cluster mode) and cluster mode. Select **Detect filer mode...**to determine which mode you have deployed.

     If you are operating in cluster mode, credentials must be set for all agents. The credentials set must be for users with ONTAPI access on the filer. Once entered, Change Auditor verifies that the specified account can access the filer. If there is an issue, re-enter valid credentials and the verification will run again.
   - **Audit Path** - Select **File** and enter a file name and path (<*ShareName*>\<*Path*>\<*FileName*>) to be audited or click the browse button to locate and select a file. Click **Add** to move the specified audit path to the selection list (middle of the page).
   - **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.

   Click **Next** to proceed to the next page.
3. On the second page of the wizard, select the agents to use to connect to the NetApp filer to capture the NetApp events.To add an agent to the NetApp Auditing template, click **Add**, select one or more agents from the list and click **OK**.
4. Click **Finish** to close the wizard and create the template.
5. On the Administration Tasks tab, click **Configuration**. Select **Agent** in the Configuration task list to open the Agent Configuration page.
6. Select the agents assigned to the template (**Auditing** appears in the **NetApp** column) 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.

To audit a folder:

1. Open the NetApp Auditing wizard. (Click **Add** or **Edit** on the NetApp Auditing page.)
2. On the first page of the wizard, enter the following information:
   - **NetApp Filer** - Select the NetApp CIFS server from the drop-down menu. If the NetApp CIFS server not appear in the list, enter the server's NetBIOS name.
   - File and folder auditing is supported in both 7-mode (non-cluster mode) and cluster mode. Select **Detect filer mode** to determine which mode you have deployed.

     If you are operating in cluster mode, credentials must be set for all agents. The credentials set must be for users with ONTAPI access on the filer.

     Once entered, Change Auditor verifies that the specified account can access the filer. If there is an issue, re-enter valid credentials and the verification will run again.

- **Audit Path** - Select **Folder** and enter a folder name and path (<*ShareName*>\<*FolderName*>) to be audited or click the browse button to locate and select a folder.

  NOTE: In order to audit changes to a share under a QTree share, you must add both the QTree share AND the share to be audited as audit paths in the NetApp Auditing template.

  For example, if you want to audit file changes when users access a share called 'folder1', which resides under a QTree share named 'c$', you need to specify the following two paths:

  - c$\folder1
  - folder1

Click **Add** to add the specified folder to the selection list.

3 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, when the folder entry is selected in the Selection list, the tabs across the bottom of the page are activated. The settings specified on these tabs apply to the entry selected.

4 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.

5 On the Inclusions tab, 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.
- A double asterisk (**) to specify a recursive match. (find match in the folder and all subfolders in audit path).

NOTE: The slash (\) and double asterisk (**) characters can only be used with volumes.

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 a subfolder, you will only receive events for operations performed against the specified subfolder. You will not receive events for operations performed against any child objects under the specified subfolder.

Once you have specified the subfolders/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.

6 (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 and path of an individual subfolder or file to be excluded.

> **IMPORTANT:** If you enter the name of a subfolder or file that is outside of the audited path, Change Auditor will not exclude it from auditing.

Once you have 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.

7 Click **Next.**

8 On the second page of the wizard, select the agents to be used to monitor the NetApp filer and click **Add.** On the Eligible Change Auditor Agents dialog, select one or more agents from the list and click **OK**.

9 Click **Finish** to close the wizard and create the template.

10 On the Administration Tasks tab, click **Configuration**. Select **Agent** in the Configuration task list to open the Agent Configuration page.

11 Select the agents assigned to the template (**Auditing** appears in the **NetApp** column) 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.

To audit a volume:

1 Open the NetApp Auditing Wizard. (Click **Add** or **Edit** on NetApp Auditing page.)

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

- **NetApp Filer** - Select the NetApp CIFS server from the drop-down menu. If the NetApp CIFS server not appear in the list, enter the server's NetBIOS name.
- File and folder auditing is supported in both 7-mode (non-cluster mode) and cluster mode. Select **Detect filer mode...**to determine which mode you have deployed.

  If you are operating in cluster mode, credentials must be set for all agents. The credentials set must be for users with ONTAPI access on the filer.

  Once entered, Change Auditor verifies that the specified account can access the filer. If there is an issue, re-enter valid credentials and the verification will run again.
- **Audit Path** - Select **Volume**. Enter a volume name (<*VolumeName*>) to be audited. Volume names can be determined by logging into the NetApp server and using the command: vol status.

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

Click **Add** to add the specified volume to the selection list (middle of the page).

3 By default, the scope of coverage for the selected volume will be **This object and all child objects**, which cannot be changed.

Select the volume entry in the Selection list to activate the tabs across the bottom of the page. The settings specified on these tabs apply to the entry selected.

4 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.

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

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.
- A double asterisk (**) to specify a recursive match. (find match in the folder and all subfolders in audit path).

  > **NOTE:** The slash (\) and double asterisk (**) characters can only be used with volumes.

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 a subfolder, you will only receive events for operations performed against the specified subfolder. You will NOT receive events for operations performed against any child objects under the specified subfolder.

Once you have specified the subfolders/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.

6 (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.

> **IMPORTANT:** If you enter the name of a subfolder or file that is outside of the audited path, Change Auditor will NOT exclude it from auditing.

Once you have 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.

7 Click **Next.**

8 On the second page of the wizard, click **Add** to select the agents to monitor the NetApp filer. On the Eligible Change Auditor Agents dialog, select one or more agents from the list and click **OK**.

9 Click **Finish** to close the wizard and create the template.

10 On the Administration Tasks tab, click **Configuration**. Select **Agent** in the Configuration task list to open the Agent Configuration page.

11 Select the Change Auditor agents assigned to the template (**Auditing** appears in the **NetApp** column) 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.

To disable an auditing template:

Disabling a template allows you to temporarily stop auditing the specified audit path without having to remove the auditing template or individual audit path from a template.

1 On the NetApp Auditing page, use one of the following methods to disable an auditing template:

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

The entry in the **Status** column for the template will change to 'Disabled'.

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

To disable the auditing of an audit path in a template:

1 On the NetApp Auditing page, use one of the following methods to disable an audit path in an auditing template:

- Place your cursor in the **Status** cell for the audit path to be disabled, click the arrow control and select **Disabled**.
- Right-click the audit 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 an audit path, use the **Enable** option in either the **Status** cell or right-click menu.

To delete an auditing template:

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

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

To delete an audit path from a template:

> **NOTE:** In Auditing templates, you cannot delete the last audit path.

1 On the NetApp page, select the audit path to be deleted and click **Delete | Delete File Path**.

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

To delete a Change Auditor agent from a template:

> **NOTE:** In Part Number or Rev Auditing templates, you cannot delete the last Change Auditor agent.

1 On the NetApp Auditing page, select the agent to be deleted and click **Delete | Delete Agent**.

2 A dialog will be displayed confirming that you want to delete the selected agent from the template. Click **Yes**.

NetApp Auditing wizard

The NetApp Auditing wizard is displayed when you click **Add** on the NetApp Auditing page. This wizard steps you through the process of creating a new NetApp auditing template, identifying the NetApp filer to audit, the auditing scope, and the agents to receive the events.

NOTE: For NetApp 7-mode, you must enable TLS communication on the filer to allow secure communication with the client using the following command: `options tls.enable on`

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

Create or modify a NetApp Auditing Template page Use the first page of the wizard to specify the NetApp filer to be audited and the file, folder, volume or all volumes to be audited on that filer.	
NetApp Filer	Use the drop-down control to the far right of this field to select the NetApp CIFS server from the drop-down menu. If the NetApp CIFS server not appear in the list, enter the server's NetBIOS name. File and folder auditing is supported in both 7-mode (non-cluster mode) and cluster mode. Select **Detect filer mode...**to determine which mode you have deployed. If you are operating in cluster mode, credentials must be set for all agents. The credentials set must be for users with ONTAPI access on the filer. Once entered, Change Auditor verifies that the specified account can access the filer. If there is an issue, re-enter valid credentials and the verification will run again. **NOTE:** There can be only one NetApp Auditing template per NetApp filer. The wizard will not allow you to create a duplicate template using the same NetApp filer name.
Audit Path	Select one of the following options to define auditing for a file, folder or volume: • **File** - select this option to audit a single file. Then enter a file name and path (<*ShareName*>\<*Path*>\<*FileName*>) to be audited or click the browse button to locate and select a file. • **Folder** - select this option to audit a folder or a set of files. Then enter a folder name and path (<*ShareName*>\<*FolderName*>) to be audited. • **Volume** - select this option to audit a single volume. Then enter the volume name (<*VolumeName*>) to be audited or click the browse button to locate and select a volume. **NOTE:** Volume names are case sensitive and must be entered correctly in the **Audit Path** field. • **All Volumes** - select this option to audit all volumes. The Audit Path text box will contain an asterisk (*) which cannot be changed. Once you have entered the audit path to be audited, click **Add** to add it to the selection list.

Table 2. NetApp Auditing wizard

...	Click the browse button to locate and select the file or folder to be audited. **NOTE:** This button is not available when **All Volumes** is selected as the audit path.
Add	Use **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 Volumes** option is selected, you must still click **Add** to move it to the selection list.
Remove	Select an entry in the selection list and click **Remove** to remove it from the list.
Selection list	The list box, located across the middle of this page, displays the files, folders or volumes 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. • **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 vital file and/or folder events.	
File Events	Select the file events to audit. Select the **File Events** check box to select all of the file events listed or select individual events from the list.
Folder Events	Select the folder events to audit. Select the **Folder Events** check box to select all of the folder events listed or select individual events from the list.
Inclusions tab	
When the **Folder**, **Volume** or **All Volumes** 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.	
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. • A double asterisk (**) to specify a recursive match. (find match in the folder and all subfolders in audit path). Note: The slash (\) and double asterisk (**) characters can only be used with volumes. For example, entering * will include all folders and files in the selected audit path. See File and Folder Inclusion and Exclusion Examples for more file mask examples. You can also enter the name of an individual subfolder or file that is to be included. However, if you enter the name of a subfolder, you will only receive events for operations performed against the specified subfolder. You will NOT receive events for operations performed against any child objects under the specified subfolder. Once you have specified the subfolders and files to be included, select **Add** to add it to the Inclusions list.

Table 2. NetApp Auditing wizard

Inclusions list	The list across the bottom of this page contains the subfolders and files selected for auditing. Use the buttons to the right of the text box to add and remove entries. • **Add** - Click **Add** 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**, **Volume** or **All Volumes** 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.	
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 and Folder Inclusion and Exclusion Examples for more examples. You can also enter the name of an individual subfolder or file that is to be excluded from auditing. If you enter the name of a subfolder or file that is outside of the audited path, Change Auditor will NOT exclude it from auditing. Once you have specified a subfolder or file to be excluded, select 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 option to exclude activity against files/subfolders in any folders that match the exclusion string. • **Add | File** - use this option to exclude activity against any files that match the exclusion string. • **Remove** - Select an entry in the Exclusions list and click **Remove** to remove it.

Table 2. NetApp Auditing wizard

Select Change Auditor Agents page	
Use this page to select the agents to receive the audit events captured on the selected NetApp filer. **NOTE:** You can improve performance by assigning a template to more than one agent. When multiple agents are assigned to the same template, events will be load balanced between these agents. However the downside is that the 'where' field for NetApp events may contain any one of these agents. In addition, if NetApp event logging is enabled, events will be written on multiple agent servers.	
Add	Use **Add** to assign one or more agents to the NetApp Auditing template. Clicking this button displays the Change Auditor Agents dialog. From this dialog, select one or more agents and then click **OK**.
Remove	Use **Remove** to remove the selected agent from the list.
Set Credentials	If you did not add the agent accounts to the local Administrators group on the NetApp filer, select the agent from the list and click **Set Credentials**. Enter the NetApp filer credentials to be used. See the Release Notes for required rights and permission.
Clear Credentials	Use **Clear Credentials** to clear the NetApp filer credentials that were previously entered for the selected agent. **NOTE:** Credentials are required when monitoring a filer in cluster mode.
Change Auditor Agent list	The list box on this page lists the agents selected to capture audit events from the selected NetApp filer.

File System events settings

From the Agent Configuration page on the Administration Tasks tab you can view and/or modify the File System settings for handling duplicate 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 Events 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 (for example, the configuration that is being used by the agents assigned to receive NetApp events).
6. Open the File System tab and set the File System Events 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 Change Auditor agents assigned to the NetApp Auditing template (**Auditing** appears in the **NetApp** column) 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.

NetApp event logging

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

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

To enable event logging:

1 Open the Administration Tasks tab.

2 Click **Configuration**.

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

4 Click **Event Logging**.

5 On the Event Logging dialog, select **NetApp**.

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

The NetApp events configured in the NetApp Auditing template will then be sent to the ChangeAuditor for NetApp event log.

4

NetApp Searches/Reports

- Introduction
- Create custom NetApp searches

Introduction

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

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

Create custom NetApp searches

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

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

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

To search for all file system events including NetApp 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 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 the **All File System Paths** option.
7. Review the Actions section and select those that are to be included in the search.

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

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

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

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

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

1 Open the Searches page.

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

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

3 Click **New** to enable the Search Properties tabs across the bottom of the Searches page.

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

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

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

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

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

- To search for events against a specific volume, enter the path as follows: \\<*FilerName*>\<*ShareName*>\
- To search for events against a specific folder, enter the path as follows: \\<*FilerName*>\<*ShareName*>\<*FolderName*>\
- To search for events against a specific file, enter the path as follows: \\<*FilerName*>\<*ShareName*>\<*FolderName*>\<*FileName.ext*>

NOTE: If the scope of your search is **This Object**, you can use the * wildcard character to specify the NetApp filer path. That is, use an asterisk (*) to substitute zero or more characters.

When using the **This Object** option, be sure to select the appropriate **Type** option to define the type of path to be searched: **Files** or **Folders**.

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

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

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

NOTE: The Transaction option does not apply to NetApp events.

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

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

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

To search for a specific NetApp event class:

1 Open the Searches page.

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

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

3 Click **New** to enable the Search Properties tabs across the bottom of the Searches page.

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

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

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

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

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

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

5

Performance Considerations

This section contains strategies to help minimize performance issues.

NOTE: Quest recommends for all environments, a phased approach to setting up file/folder auditing for NetApp devices. A phased approach will allow file/folder auditing to be deployed in stages so that performance is not impacted.

- Change Auditor agent performance
- Configuring audit scope

Change Auditor agent performance

Performance is directly linked to the CPU speed and network latency of the server hosting the agent collecting the NetApp events.

- Hardware considerations
- Load balancing

Hardware considerations

To improve agent performance, you can:

- Upgrade the link between the NetApp filer and the agent to decrease network latency.
- Add extra CPUs to the current agent or select a more powerful agent host with more CPUs or CPU cores available.

See the Release Notes for required rights and permission.

Load balancing

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

NOTE: Only increase the number of agents if a single agent cannot handle the volume of events generated.

NOTE: For NetApp filers generating a large amount of events, it is recommended that you do NOT assign the same agents to multiple filers (NetApp Auditing templates).

NOTE: An ONTAP 7.2 filer can be audited by one or more agents for load balancing of events, but the same agents cannot audit more than one ONTAP 7.2 filer.

Configuring audit scope

Audit only volumes, extensions and operations that are vital for your environment. Use the NetApp auditing template to specify the auditing scope for a NetApp filer. For example, using the NetApp Auditing template you can:

- Decrease the number of volumes being audited
  - Set the Audit Path to **File**, **Folder** or **Volume** and enter the file, folder or volume to be audited.
    - To specify a file, enter: <*ShareName*>\<*Path*>\<*FileName*>
    - To specify a folder, enter: <*ShareName*>\<*FolderName*>
    - To specify a volume, enter: <*VolumeName*>

    NOTE: Specifying a volume name provides the best performance.

- Decrease the number of file extensions being audited
  - Use the Inclusions tab to specify individual subfolders or files to be included for auditing.

    NOTE: For better performance, on the Inclusions tab specify only three characters for included extensions (e.g., *.txt, *.x??).

  - Use the Exclusions tab to exclude individual subfolders or files from auditing.

  NOTE: On both the Inclusions and Exclusions tabs, you can specify a group of files or subfolders using wildcard characters. That is, use an asterisk (*) to substitute zero or more characters or use a question mark (?) to substitute a single character.

  See File and Folder Inclusion and Exclusion Examples for more information and examples.

- Decrease the number of operations being audited
  - Use the Events tab to select only vital file and/or folder events.

6

NetApp Filer Events

The following events can be selected for auditing from the Events tab on the NetApp 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

- NetApp File access rights changed (no from-value)
- NetApp File contents written
- NetApp File created
- NetApp File deleted
- NetApp File moved
- NetApp File opened (Only available when Audit Path is File)
- NetApp File ownership changed (no from-value)
- NetApp File renamed

Folder Events

- NetApp Folder access rights changed (no from-value)
- NetApp Folder created
- NetApp Folder deleted
- NetApp Folder moved
- NetApp Folder ownership changed (no from-value)
- NetApp Folder renamed

7

File and Folder Inclusion and Exclusion Examples

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

The Inclusions and Exclusions tabs only appear when the **Folder**, **Volume** or **All Volumes** 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.
- A double asterisk (**) to specify a recursive match. (find match in the folder and all subfolders in audit path).

NOTE: The slash (\) and double asterisk (**) characters can only be used with volumes.

Examples:

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

Table 3. Inclusion examples

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

Table 3. Inclusion examples

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

Exclusions tab

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

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

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

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

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

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

Exclusion examples

These examples show how to use file masks on the Exclusions tab of the auditing wizard. Note that <*String*> in these examples may contain any of the file mask characters described above (such as, fixed characters, * or ?).

- Folder exclusion examples
- Volume exclusion examples
- All volume exclusion examples

Folder exclusion examples

Audit Path = Folder (<ShareName>\<FolderName>) exclusion examples

In the following examples the Audit Path is HOME\TEMP.

Table 4. 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:** HOME\TEMP\DOCS
Exclude activity against files/subfolders in all folders that contain a specific string in their name, which are located in the base audit path. (**Add | Folder**)	**Exclusion Syntax:** <*FolderNameString*> **Example 1:** DOC* **Excludes:** HOME\TEMP\DOCS HOME\TEMP\DOCUMENTS **Example 2:** *DOC **Excludes:** HOME\TEMP\MYDOC **Example 3:** *DOC? **Excludes:** HOME\TEMP\DOCS HOME\TEMP\MYDOCX HOME\TEMP\PUBLICDOCS
Exclude activity against files/subfolders in all folders with a specific name found anywhere in the audit path. (**Add | Folder**)	**Exclusion Syntax:** **\<*FolderName*> **Example:** **\MYDOC **Excludes:** HOME\TEMP\MYDOC HOME\TEMP\DOCUMENTS\MYDOC HOME\TEMP\DOCS\PRIVATE\MYDOC
Exclude activity against a specific file in the base audit path. (**Add | File**)	**Exclusion Syntax:** <*FileName.ext*> **Example:** Test1.docx **Excludes:** HOME\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:** HOME\TEMP\Doc1.tmp HOME\TEMP\Testing123.tmp

Table 4. Exclusion examples: Audit Path = Folder

What to exclude	Exclusion syntax/examples
Exclude activity against all files with a specific file extension, which may be found anywhere in the audit path. (**Add | File**)	**Exclusion Syntax:** **.<*ext*> **Example:** **.tmp **Excludes:** HOME\TEMP\Doc1.tmp HOME\TEMP\DOCUMENTS\Testing.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. HOME\TEMP\Myword.doc HOME\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'. HOME\TEMP\Word.tmp HOME\TEMP\Mywordtest.tmp HOME\TEMP\Nowords.bmp

Volume exclusion examples

Audit Path = Volume (<VolumeName>) exclusion examples

In the following examples, the volume name is Vol0 (Audit Path = Vol0); share names are HOME, SHARE2, and SHAREDDOCS.

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

NOTE: When auditing an individual volume or all volumes, you must include the share name (or a file mask to represent the share) in the exclusion path.

NOTE: If a file exclusion is added that does not include a slash (\), it will be automatically appended with "*.*".

Table 5. Exclusion examples: Audit Path = Volume

What to exclude	Exclusion syntax/examples
Exclude activity against files/subfolders in a specific folder found in a specific location on the selected volume. (**Add | Folder**)	**Exclusion Syntax:** <*ShareName*>\<*Path*>\<*FolderName*> **Example:** HOME\USERS\TEMP\DOCS **Excludes:** Vol0\HOME\USERS\TEMP\DOCS
Exclude activity against files/subfolders in all folders whose name contains a specific string of characters found in a specific location on the selected volume. (**Add | Folder**)	**Exclusion Syntax:** <*ShareName*>\<*Path*>\<*CharString*> **Example:** HOME\USERS\TE?????DOCS **Excludes:** Vol0\HOME\USERS\TESTINGDOCS Vol0\HOME\USERS\TEMPORARYDOCS
Exclude activity against files/subfolders in all folders with the specified folder name which is located on a specific share. (**Add | Folder**)	**Exclusion Syntax:** <*ShareName*>**\<*FolderName*> **Example:** HOME**\DOCS **Excludes:** Vol0\HOME\DOCS Vol0\HOME\DEPTS\DOCS Vol0\HOME\USERS\TEMP\DOCS
Exclude activity against files/subfolders in all folders whose name starts with a specific string of characters which are located on a specific share. (**Add | Folder**)	**Exclusion Syntax:** <*ShareName*>**\<*CharString*>* **Example:** HOME**\DOC* **Excludes:** Vol0\HOME\DOCS Vol0\HOME\DEPTS\DOCS Vol0\HOME\USERS\TEMP\DOCS Vol0\HOME\USERS\DOCUMENTS
Exclude activity against files/subfolders in all folders with the specified folder name found in a specific path level on all shares on the selected volume. (**Add | Folder**)	**Exclusion Syntax:** **\<*FolderName*> **Example 1:** **\DOCS **Excludes:** Vol0\HOME\USERS\DOCS Vol0\HOME\DEPTS\DOCS Vol0\SHARE2\TEST\DOCS Example 2: ***\DOCS Excludes: Vol0\HOME\USERS\TEMP\DOCS Vol0\SHARE2\PUBLIC\TEST\DOCS
Exclude activity against files/subfolders in all folders with the specified folder name which may be located anywhere on the selected volume. (**Add | Folder**)	**Exclusion Syntax:** **\<*FolderName*> **Example:** **\DOCS **Excludes:** Vol0\HOME\DOCS Vol0\HOME\DEPTS\DOCS Vol0\HOME\USERS\TEMP\DOCS Vol0\SHARE2\TEST\DOCS Vol0\SHARE2\PUBLIC\TEST\DOCS

Table 5. Exclusion examples: Audit Path = Volume

What to exclude	Exclusion syntax/examples
Exclude activity against files/subfolders in all shares and folders whose name contains a specific string of characters which may be located anywhere on the selected volume. (**Add | Folder**)	**Exclusion Syntax:** **<*CharString*>* **Example:** **DOC* **Excludes:** Vol0\HOME\DOCS Vol0\HOME\MYDOCS Vol0\HOME\USERS\TEMP\DOCS Vol0\HOME\USERS\TEMPORARYDOCS Vol0\SHARE2\TEST\DOCS Vol0\SHARE2\PUBLIC\TEST\MYDOCS Vol0\SHAREDDOC
Exclude activity against files whose name contains a specific string of characters which may be found anywhere on the selected volume. (**Add | File**)	**Exclusion Syntax**: ***<CharString>* **Example**: ***DOC* **Excludes**: Vol0\HOME\Document1.tmp Vol0\HOME\FILES\Testing.doc Vol0\HOME\USERS\TEMP\FILES\BetaDoc.pdf Vol0\SHARE2\USERS\DECEMBER\Test1.docx Vol0\SHARE2\PUBLIC\MARCH\OldDocPlan
Exclude activity against a specific file found in a specific location on the selected volume. (**Add | File**)	**Exclusion Syntax:** <*ShareName*>\<*Path*>\<*FileName.Ext*> **Example:** SHARE2\USERS\DOCS\Test1.docx **Excludes:** Vol0\SHARE2\USERS\DOCS\Test1.docx
Exclude activity against files with a specific file name (regardless of the file extension) which may be located anywhere on the selected volume. (**Add | File**)	**Exclusion Syntax:** **\<*FileName*>.* **Example:** **\test1.* **Excludes:** Vol0\HOME\DEPTS\DOCS\test1.docx Vol0\HOME\USERS\TEMP\DOCS\test1.docx Vol0\HOME\USERS\DOCUMENTS\test1.pdf Vol0\SHARE2\TEST\DOCS\test1.txt
Exclude activity against files with the specified file extension found in a specific location on the selected volume. (**Add | File**)	**Exclusion Syntax:** <*ShareName*>\<*Path*>*.<*Ext*> **Example:** SHARE2\TEST\DOCS*.docx **Excludes:** Vol0\SHARE2\TEST\DOCS\Test1.docx Vol0\SHARE2\TEST\DOCS\MyInfo.docx
Exclude activity against files with the specified file extension which may be located anywhere on the selected volume. (**Add | File**)	**Exclusion Syntax:** ***.<*Ext*> **Example:** ***.pdf **Excludes:** Vol0\HOME\MYDOCS\Final.pdf Vol0\HOME\DEPTS\DOCS\Test123.pdf Vol0\HOME\USERS\DOCUMENTS\Test1.pdf Vol0\SHARE2\TEST\DOCS\Current.pdf Vol0\SHARE2\PUBLIC\TEST\MYDOCS\Ex.pdf

All volume exclusion examples

Audit Path = All Volumes exclusion examples

In the following examples, Vol0 contains three shares: HOME, SHARE2 and SHAREDDOCS; and Vol1 contains one share: SHAREDAPPS.

NOTE: When using **All Volumes**, you cannot exclude an individual volume. You must use a share name, which is unique to a volume. That is, you cannot have two shares with the name of HOME (either on the same volume or different volumes).

NOTE: When auditing an individual volume or all volumes, you must include the share name (or a file mask to represent the share) in the exclusion path.

Table 6. Exclusion examples: Audit Path = All Volumes

What to exclude	Exclusion syntax/examples
Exclude activity against files/subfolders in a specific folder found in a specific location on all volumes. (**Add | Folder**)	**Exclusion Syntax:** *\<*Path*>\<*FolderName*> **Example:** *\USERS\TEMP\DOCS **Excludes:** Vol0\HOME\USERS\TEMP\DOCS Vol0\SHARED2\USERS\TEMP\DOCS Vol1\SHAREDAPPS\USERS\TEMP\DOCS
Exclude activity against files/subfolders in all folders with the specified folder name found on a specific share. (**Add | Folder**)	**Exclusion Syntax:** <*ShareName*>**\<*FolderName*> **Example:** HOME**\DOCS **Excludes:** Vol0\HOME\DOCS Vol0\HOME\DEPTS\DOCS Vol0\HOME\USERS\TEMP\DOCS
Exclude activity against files/subfolders in all folders whose name starts with a specific string of characters found on a specific share. (**Add | Folder**)	**Exclusion Syntax:** <*ShareName*>**\<*CharString*>* **Example:** HOME**\DOC* **Excludes:** Vol0\HOME\DOCS Vol0\HOME\DEPTS\DOCS Vol0\HOME\USERS\TEMP\DOCS Vol0\HOME\USERS\DOCUMENTS
Exclude activity against files/subfolders in all folders with the specified folder name found anywhere on all volumes. (**Add | Folder**)	**Exclusion Syntax:** **\<*FolderName*> **Example:** **\DOCS **Excludes:** Vol0\HOME\DOCS Vol0\HOME\DEPTS\DOCS Vol0\HOME\USERS\TEMP\DOCS Vol0\SHARE2\TEST\DOCS Vol1\SHAREDAPPS\DOCS

Table 6. Exclusion examples: Audit Path = All Volumes

What to exclude	Exclusion syntax/examples
Exclude activity against files/subfolders in all folders with the specified folder name found at a specific level on all volumes. (**Add | Folder**)	**Exclusion Syntax:** **\<*FolderName*> **Example 1:** **\DOCS **Excludes:** Vol0\HOME\DEPTS\DOCS Vol0\SHARE2\TEST\DOCS Vol1\SHAREDAPPS\INSTALL\DOCS **Example 2:** ***\DOCS **Excludes:** Vol0\HOME\USERS\TEMP\DOCS Vol0\SHARED2\PUBLIC\TEST\DOCS Vol1\SHAREDAPPS\PROCS\INTRO\DOCS
Exclude activity against files/subfolders in all shares and folders whose name ends with a specific string of characters that may be located anywhere on all volumes. (**Add | Folder**)	**Exclusion Syntax:** **<*CharString*> **Example:** **DOCS **Excludes:** Vol0\HOME\DOCS Vol0\HOME\MYDOCS Vol0\HOME\USERS\TEMP\DOCS Vol0\HOME\USERS\TEMPORARYDOCS Vol0\HOME\USERS\TEMP\TESTINGDOCS Vol0\SHARE2\TEST\DOCS Vol0\SHARE2\PUBLIC\TEST\DOCS Vol0\SHAREDDOCS Vol1\SHAREDAPPS\INSTALL\DOCS Vol1\SHAREDAPPS\PROCS\INTRO\DOCS
Exclude a specific file found in a specific location on the specified share. (**Add | File**)	**Exclusion Syntax:** <*ShareName*>\<*Path*>\<*FileName.Ext*> **Entering:** SHARE2\USERS\DOCS\Test1.docx **Excludes:** Vol0\SHARE2\USERS\DOCS\Test1.docx
Exclude activity against all files with the specified file extension found in a specific location on the specified share. (**Add | File**)	**Exclusion Syntax:** <*ShareName*>\<*Path*>*.<*Ext*> **Entering:** SHARE2\TEST\DOCS*.docx **Excludes:** Vol0\SHARE2\TEST\DOCS\Test1.docx Vol0\SHARE2\TEST\DOCS\123testing.docx
Exclude activity against all files with the specified file extension found anywhere on all volumes. (**Add | File**)	**Exclusion Syntax:** ***.<*Ext*> **Example:** ***.pdf **Excludes:** Vol0\HOME\DEPTS\DOCS\Test123.pdf Vol0\SHARE2\TEST\DOCS\Current.pdf Vol1\SHAREDAPPS\WhatsNew.pdf
Exclude a specific file (regardless of the file extension) found anywhere on the all volumes. (**Add | File**)	**Exclusion Syntax:** **\<*FileName*>.* **Entering:** **\test1.* **Excludes:** Vol0\HOME\DEPTS\DOCS\test1.docx Vol0\HOME\USERS\TEMP\DOCS\test1.docx Vol0\HOME\USERS\DOCUMENTS\test1.pdf Vol0\SHARE2\USERS\DOCS\test1.txt Vol1\SHAREDAPPS\test1.xlsx

About us

Quest provides software solutions for the rapidly-changing world of enterprise IT. We help simplify the challenges caused by data explosion, cloud expansion, hybrid datacenters, security threats, and regulatory requirements. We are a global provider to 130,000 companies across 100 countries, including 95% of the Fortune 500 and 90% of the Global 1000. Since 1987, we have built a portfolio of solutions that now includes database management, data protection, identity and access management, Microsoft platform management, and unified endpoint management. With Quest, organizations spend less time on IT administration and more time on business innovation. 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.