Quest®Change Auditor for EMC® 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 EMC User Guide
Updated - August 2026
Software Version - 7.6.3

Contents

Quest Change Auditor for EMC Overview 5
Introduction 5
System overview 6
Deployment requirements 7
Client components and features 8

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

EMC Auditing 11
Introduction 11
EMC Auditing page 11
EMC auditing templates 13
EMC Auditing wizard 20
File System events settings 25
EMC event logging 25

EMC Searches/Reports 27
Introduction 27
Create custom EMC searches 27

Performance Considerations 30
Change Auditor agent performance 30
Hardware considerations 30
Load balancing 30
Configuring audit scope 31

EMC Events 32

File/Folder Inclusion and Exclusion Examples 33
Inclusions tab 33
Exclusions tab 35

EMC Isilon Auditing 42
Configuration Notes 42

EMC Unity Auditing 45
Configuration Notes 45

About us 46
Our brand, our vision. Together. 46
Contacting Quest 46

Technical support resources 46

1

Quest Change Auditor for EMC Overview

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

Introduction

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

Quest Change Auditor for EMC captures events and provides detailed information relating to the following activities:

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

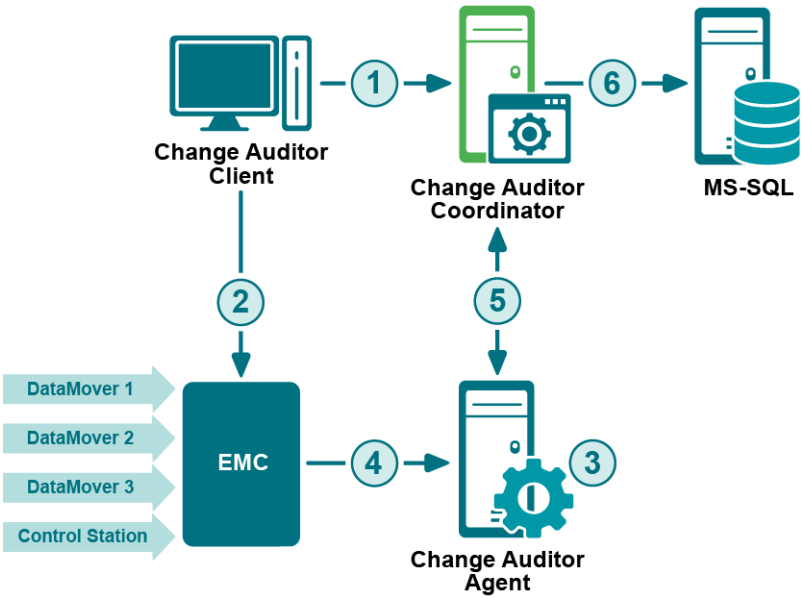
NOTE: Change Auditor only captures EMC events initiated through a Common Internet File System (CIFS). EMC events initiated through FTP, NFS, or other protocols are not captured.

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

System overview

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



1 Using the client, users create an EMC Auditing template to configure the EMC file server (CIFS) location and select the agent to receive the EMC events.

   The coordinator is responsible for fulfilling client and agent requests.

2 (Optional) The client updates the EMC Control Station to enable auditing using an updated cepp.conf file (optional step in the EMC Auditing wizard).

3 The agent registers with the EMC CEE/VEE Framework service to get data related to user operations.

4 The EMC Data Mover forwards audit events to the EMC CEE/VEE Framework installed on the Change Auditor agent server.

5 The agent processes EMC events and forwards them to the coordinator.

6 The coordinator forwards the events and related details to the database.

Deployment requirements

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

To audit EMC, you need to:

- Install EMC Event Enabler Framework
- Create EMC Auditing template

Install EMC Event Enabler Framework

NOTE: This guide outlines the installation steps that are required for Change Auditor to integrate with the EMC Event Enabler Framework. For detailed installation steps, see the appropriate guides from EMC Corporation. See the EMC Corporation website (http://www.emc.com/) for information about downloading EMC product executables.

1. Download the Common Event Enabler (CEE) Framework compatible with your device from the EMC website and install on one or more Windows servers where you want to monitor activity. The server must also have an agent installed.
2. Install the EMC Common Event Publishing Agent (CEPA) Auditing which enables Change Auditor to monitor the file system activity on EMC.

   NOTE: For Isilon or Unity NAS servers, the installation process is complete. Skip the next two steps.

   NOTE: Quest Change Auditor for EMC does not support automatic Isilon of Unity auditing configuration. See EMC Isilon Auditing and EMC Unity Auditing for more information about the manual configuration required.
3. Create a configuration file (cepp.conf file) before using the CEPA auditing feature. The cepp.conf file contains the information to connect Data Movers to the Windows computers where the CEE software is installed. You can either manually create the cepp.conf file or use Change Auditor to create this configuration file later.
4. If you manually created the cepp.conf file, start the CEPA facility and then verify that it has started. Use the following command syntax to start the CEPA facility and to check its status:
   - $ server_cepp <*DataMoverName*> -service -start
   - $ server_cepp <*DataMoverName*> -service -status

Create EMC Auditing template

You need to define an EMC auditing template for each EMC file server (CIFS) to be audited. In addition to defining the EMC file server (CIFS) to audit and the agents to receive these events, completing this step also installs the Shared EMC Connector service (QCeeService). This service enables auditing of EMC devices by multiple Quest software products. This service is required because EMC supports only one auditing pool at a time.

NOTE: The cepp.conf file contains the information to connect Data Movers to the Windows computers where the CEE is installed and stores the auditing configuration. If you manually created the cepp.conf, you can update the configuration file during template creation. More specifically, it adds a ‘quest servers’ pool name entry to the existing configuration file specifying the Change Auditor agents assigned to receive the EMC events.

NOTE: Ensure that the servers that you deploy agents to have CEPA Auditing installed.

Client components and features

The following table lists the client components and features that require a valid Quest Change Auditor for EMC license. You are not prevented from using these features; however, associated events are not 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), select **Action | Hide Unlicensed Components**. This command is only available when the Administration Tasks tab is the active page.

Table 1. Quest Change Auditor for EMC client components and features

Client page	Feature
Administration Tasks Tab	Agent Configuration Page: • Event Logging - enable/disable EMC event logging **NOTE:** See EMC event logging for information about enabling EMC event logging. • Configuration Setup Dialog - File System Tab ▪ Discard duplicates that occur within nn seconds ▪ Audit all configured, including duplicates (Not Recommended) **NOTE:** See File System events settings for details about these File System Events settings. Audit Task List: • EMC **NOTE:** See EMC auditing templates for information about creating templates to define EMC auditing.
Event Details Pane	What Details: • Path • Process
Events	Facilities: • EMC
Search Properties	What Tab: • Subsystem | File System **NOTE:** See Create custom EMC searches for information about using the What tab to create custom EMC search queries.
Searches Page	Built-in Reports: • Reports that include EMC events

2

Getting Started

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

Introduction

This section provides a high-level view of the tasks to get you started using Quest Change Auditor for EMC. It assumes you have successfully installed/licensed Quest Change Auditor for EMC and the EMC Common Event Enabler (CEE) Framework.

NOTE: EMC auditing is only available if you have licensed Quest Change Auditor for EMC. 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 EMC events are being captured, check to see if the agent assigned to the EMC 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. Select **View | Administration**.
3. If not already selected, click **Configuration**.
4. Select **Agent** in the Configuration task list to open the Agent Configuration page.
5. Select the agent assigned to the EMC Auditing template (**Auditing** appears in the **EMC** column) and click **Refresh Configuration**.

Make changes and run a report

1. To test EMC auditing, make changes to the EMC NAS being monitored.

   For example:

   - create a new folder
   - add a new .txt or .docx file in this folder
   - change the security permissions on a file (right-click file, open the Security tab and add another user with full control)

- delete the sample .txt file
- add a sub-folder
- change the security permission of the new folder

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

3 Open the Searches tab.

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

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

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

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

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

Troubleshooting steps

If the EMC events do not appear in the client as expected, check the following:

- Verify that the CEPA (EMC CAVA agent service) is running on the Windows Server where the EMC events are being collected.
- Verify that the Shared EMC Connector service (QCeeService) is running.
- Use the following command to verify that the CEPP service on the EMC Data Mover is running and is in the state of ONLINE:

  server_cepp <*DataMoverName*> -p -i

  If the CEPP service is OFFLINE, restart the EMC CAVA agent service on the Windows Server. If that does not work, restart the EMC CEPP service on the Data Mover using the following commands:

  server_cepp <*DataMoverName*> -service -stop
  server_cepp <*DataMoverName*> -service -start
- Verify that the EMC file server (CIFS) is valid on the first page of the EMC Auditing wizard. The **EMC File Server (CIFS)** field should contain the IP address or Netbios name of the CIFS to be audited.
- Verify that you have selected those type of events in the EMC Auditing template. (Events tab in wizard.)
- Verify that you have included the correct subfolders and paths in the EMC Auditing template. (Inclusions tab in wizard.)

  NOTE: Entering * will include all subfolders and paths.
- Verify that you have not excluded the specified subfolders or paths in the EMC Auditing template. (Exclusions tab in wizard.)
- If you set the credentials on the second page of the wizard, verify that you have selected the correct Data Mover for the selected CIFS.
- Refresh the specified agent configurations on the Agent Configuration page to ensure the latest EMC Auditing template is being used.

3

EMC Auditing

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

Introduction

You must define a separate EMC Auditing template for each EMC file server (CIFS) to audit. The EMC Auditing page on the Administration Tasks tab displays details about each EMC Auditing template created and allows you to add new auditing templates.

This section provides a description of the EMC Auditing page and EMC 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.

EMC Auditing page

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

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

The EMC Auditing page contains an expandable view of all the EMC 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:

File Server (CIFS)

Displays the name of the EMC file server (CIFS) specified in the wizard.

Status

Indicates whether the auditing template is enabled or disabled.

Paths

This field is used for filtering data.

Audit cepp.conf

Indicates whether you have selected to audit the cepp.conf file for changes made by other third-party applications.

NOTE: This field does not apply to Isilon file server auditing.

Auditing Agent

Displays the name of the agent assigned to audit the cepp.conf file.

NOTE: This field will be blank if the **Audit cepp.conf** field is set to **No**.

Polling Interval Minutes

Displays the polling interval specified when auditing of the cepp.conf file is enabled.

NOTE: This field will be blank if the **Audit cepp.conf** field is set to **No**.

NOTE: This field does not apply to Isilon file server auditing.

Click the expansion box to the left of the EMC file server (CIFS) name to expand this view and display the following details:

Path

Displays the name of the audit paths included in the EMC 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 agents assigned to receive the EMC events from the selected EMC file server (CIFS).

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.

EMC auditing templates

To enable EMC auditing, create a template for each EMC file server (CIFS) to audit. Each template defines the location of the EMC file server to be audited, the auditing scope, and the agents to receive the events.

NOTE: There can be only one EMC Auditing template per EMC file server (CIFS). To audit multiple audit paths, use the same template to specify all the audit paths to be audited on the selected EMC file server.

NOTE: **Auditing file contents written event on EMC Isilon**:
To audit the "File contents written" operations, you must audit "Close" operations on Isilon. To audit close operations, use isi zone zones modify command in the command line interface (CLI).

For example:
To audit a successful close operation for the 'System' zone run the following command:
isi zone zones modify system --add-audit-success close.

To review all currently audited operations for the System zone, use the following command:
isi zone zones view system

To audit a file:

1. Select **View | Administration**.
2. Select **Auditing**.
3. Select **EMC** in the **Auditing | NAS** task list to open the EMC Auditing page.
4. Click **Add**.

   This opens the EMC Auditing wizard, which steps you through the process of defining the EMC file server (CIFS) to be audited, the auditing scope, and the agents that are to receive the EMC events.
5. Enter the following information:

   - **EMC File Server (CIFS)** - Select the EMC file server (CIFS) from the drop-down list. Or enter the Netbios name or IP address of the EMC file server (CIFS) to be audited.

     NOTE: When creating a template for Isilon, you must use the FQDN. If you select the NetBios name or IP address, the template will not function.

   - **Audit Path** - Select **File**. Enter a file name and path (i.e., <*ShareName*>\<*Path*>\<*FileName*>) to audit or click the browse button to locate and select a file. Click **Add** to move the specified audit path to the selection list.

     NOTE: **Isilon file server auditing**

     When specifying a file path to audit, use the file's absolute path. Path values in Isilon events captured by Change Auditor are also represented in absolute paths. For example, if a share called 'MyTestShare' is sharing the path '\\isilon\ifs\test', and you want to audit the file MyDoc.docx inside that share, add the path 'ifs\test\MyDoc.docx' in the auditing template.

     Change Auditor uses the default 'ifs' share for Isilon file/folder permission change events. If you have renamed this share, specify the new share name to continue support for these events. To change the default ifs share name, click the "Isilion admin share name" link on the top right corner of the page.

     Volume auditing is not supported and should not be used. Select **File** or **Folder** as the Audit Path.

   - **Events tab** - Select the file events to audit 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 Click **Next**.

7 On the second page of the wizard, select the agents used to connect to the EMC file server to capture the EMC events.

> **TIP:** Specifying multiple agents may provide better performance because the EMC server will load balance audit events and send each assigned agent events round-robin style. However, the downside is that the 'where' field for EMC events may contain any one of these agents. Also, if EMC event logging is enabled, events will be written on multiple agent servers.

To add an agent to the EMC Auditing template:

- Click **Add.**
- Select one or more agents from the list and click **OK**.

If the agents that are to capture EMC events are not already specified in the cepp.conf file (pool namesakes servers entry), you will need to enter the credentials required to access the EMC Control Station.

> **NOTE: Isilon file server auditing:** There is no need to enter the EMC Control Station credentials when configuring auditing on an Isilon server. Skip to Step 9.

Click **Set Credentials** and enter the following information:

- **Control Station** - enter the IP address of the EMC Control Station.
- **User** - enter the user name of an account with Administrative rights (required to create or modify the cepp.conf file) on the selected EMC Control Station.
- **Password** - enter the password associated with the user name entered above.
- **Data Mover** - select the data mover that hosts the CIFS file server specified on the first page of the wizard.

Click **Test** to validate the credentials. Once the credentials are validated, click **OK** to set the credentials as entered and close the dialog.

The cepp.conf file will be created based on the information specified in the EMC Auditing wizard. Click **Next** to view the current and proposed settings for the cepp.conf file.

8 On the last page of the wizard, review the proposed cepp.conf file, which is displayed in the bottom pane.

Use the buttons above the **Current cepp.conf File** text box, as described below:

- To deploy the proposed configuration file, click **Update File**.
- To check the current status of the cepp service, click **Check Status**.
- To audit the cepp.conf file checking for modifications made by another application, click **Audit File**. Select the **Enable Auditing** check box, review (and if necessary change) the polling interval, and select the Change Auditor agent to be used to poll this configuration file. Click **OK** to save your selections and close the dialog.

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

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

11 To ensure the agents are using the latest configuration, select the Change Auditor agents assigned to the EMC Auditing template (**Auditing** appears in the **EMC** 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 Select **View | Administration**.

2 Select **Auditing**.

3 Select **EMC** in the **Auditing | NAS** task list to open the EMC Auditing page.

4 Click **Add**.

5 Enter the following information:

- **EMC File Server (CIFS)** - Select the EMC file server (CIFS) from the drop-down list. Or enter the Netbios name or IP address of the EMC file server (CIFS) to be audited.
- **Audit Path** - Select **Folder**. Enter a folder name and path (i.e., <*ShareName*>\<*FolderName*>) to audit or click the browse button to locate and select a folder.

> **NOTE: Isilon file server auditing:**
>
> When specifying file and folder paths to be audited, the file or folder's absolute path should be used. Path values in Isilon events captured by Change Auditor are also represented in absolute paths. For example, if a share called 'MyTestShare' is sharing the path '\\isilon\ifs\test', add the path 'ifs\test' in the auditing template to audit changes through the share.
>
> Change Auditor uses the default 'ifs' share for Isilon file/folder permission change events. If you have renamed this share, please specify the new share name on this page to continue support for these events. To change the default ifs share name, click the "Isilion admin share name" link on the top right hand corner of the page.

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

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, 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.

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 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 to be included, click the **Add** button 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.

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.

Click **Next.**

10 On the second page of the wizard, select the Change Auditor agents to be used to monitor the EMC file server.

- Click **Add**.
- On the Eligible Change Auditor Agents dialog, select one or more agents from the list and select **OK**.

If the Change Auditor agents that are to capture EMC events are not already specified in the cepp.conf file (pool name=quest servers entry), you will need to enter the credentials to be used to access the EMC Control Station.

NOTE: Isilon file server auditing: There is no need to enter the EMC Control Station credentials when configuring auditing on an Isilon server. Skip to Step 12.

Click the **Set Credentials** button and enter the following information:

- **Control Station** - enter the IP address of the EMC Control Station.
- **User** - enter the user name of an account with Administrative rights (rights to create or modify the cepp.conf file) on the selected EMC Control Station.
- **Password** - enter the password associated with the user name entered above.
- **Data Mover** - select the data mover that hosts the CIFS file server specified on the first page of the wizard.

Click **Test** to validate the credentials entered. Once the credentials are validated, select **OK** to set the credentials as entered and close the dialog.

The required cepp.conf file will be created based on the information specified in the EMC Auditing wizard. Click **Next** to view the current and proposed settings for the cepp.conf file.

11 On the last page of the wizard, review the proposed cepp.conf file, which is displayed in the bottom pane.

Use the buttons above the **Current cepp.conf File** text box, as described below:

- To deploy the proposed configuration file, click **Update File**.
- To check the current status of the cepp service, click **Check Status**.
- To audit the cepp.conf file checking for modifications made by another application, click **Audit File**. Select the **Enable Auditing** check box, review (and if necessary change) the polling interval, and select the Change Auditor agent to be used to poll this configuration file. Click **OK** to save your selections and close the dialog.

12 Click **Finish** to close the wizard and create the EMC Auditing template.

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

14 Select the agents assigned to the EMC Auditing template (**Auditing** appears in the **EMC** column) 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 audit a volume:

> **NOTE: Isilon file server auditing:** Volume auditing is not support and should not be used.

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

2 Enter the following information:

- **EMC File Server (CIFS)** - Select the EMC file server (CIFS) from the drop-down list. Or enter the Netbios name or IP address of the EMC file server (CIFS) to be audited.
- **Audit Path** - Select **Volume**. Enter a volume name (i.e., <*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.

Click **Add** to add the specified volume to the Selection list.

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 to be included, 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 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.

Click **Next.**

7 On the second page of the wizard, select the Change Auditor agents to monitor the EMC file server.

- Click **Add**.
- On the Eligible Change Auditor Agents dialog, select one or more agents from the list and click **OK**.

If the Change Auditor agents that are to capture EMC events are not already specified in the cepp.conf file (pool name=quest servers entry), you'll need to enter the credentials to be used to access the EMC Control Station.

Click **Set Credentials** and enter the following information:

- **Control Station** - enter the IP address of the EMC Control Station.
- **User** - enter the user name of an account with Administrative rights (rights to create or modify the cepp.conf file) on the selected EMC Control Station.
- **Password** - enter the password associated with the user name entered above.

- **Data Mover** - select the data mover that hosts the CIFS file server specified on the first page of the wizard.

Click **Test** to validate the credentials. Once the credentials are validated, click **OK** to set the credentials as entered and close the dialog.

The required cepp.conf file will be created based on the information specified in the EMC Auditing wizard. Click **Next** to view the current and proposed settings for the cepp.conf file.

8 On the last page of the wizard, review the proposed cepp.conf file, which is displayed in the bottom pane.

Use the buttons above the **Current cepp.conf File** text box, as described below:

- To deploy the proposed configuration file, click **Update File**.
- To check the current status of the cepp service, click **Check Status**.
- To audit the cepp.conf file checking for modifications made by another application, click **Audit File**. Select the **Enable Auditing** check box, review (and if necessary change) the polling interval, and select the Change Auditor agent to be used to poll this configuration file. Click **OK** to save your selections and close the dialog.

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. This will ensure the agents are using the latest configuration.

11 Select the Change Auditor agents assigned to the EMC Auditing template (**Auditing** appears in the **EMC** 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:

The disable feature 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 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 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 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 an audit path from a template:

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

1. On the Auditing page, select the audit 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**.

To delete a Change Auditor agent from a template:

NOTE: In Auditing templates, you cannot delete the last agent.

1. On the Auditing page, select the agent to be deleted and click **Delete | Delete Agent**.
   - Right-click the agent to be deleted and select **Delete**.
2. A dialog will be displayed confirming that you want to delete the selected agent from the template. Click **Yes**.

EMC Auditing wizard

The EMC Auditing wizard displays when you click **Add** on the EMC Auditing page. This wizard steps you through the process of creating a new EMC auditing template, specifying the EMC file server (CIFS) to be audited, the auditing scope and the agents to receive events.

The following table provides a description of the fields and controls in the EMC 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 1. EMC Auditing wizard

Create or modify an EMC Auditing Template page: On the first page of the wizard, specify the EMC file server (CIFS) to auditand define the auditing scope.	
EMC File Server (CIFS)	Select the EMC file server (CIFS) from the list or enter the name of the EMC file server to audit. **NOTE:** The drop-down list contains the CIFS servers published in Active Directory. **NOTE:** Isilon servers are not listed in the drop-down list but can be entered manually.

Table 1. EMC Auditing wizard

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*>) or click 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. Then enter a folder name and path (<*ShareName*>\<*FolderName*>) or click the browse button to locate and select the folder to be audited. **NOTE: Isilon file server auditing:** When specifying a file path to be audited, you should use the file's absolute path. Path values in Isilon events captured by Change Auditor are also represented in absolute paths. For example, if a share called 'MyTestShare' is sharing the path '\\isilon\ifs\test', and you want to audit the file MyDoc.docx inside that share, add the path 'ifs\test\MyDoc.docx' in the auditing template. **NOTE:** Change Auditor uses the default 'ifs' share for Isilon file/folder permission change events. If you have renamed this share, please specify the new share name on this page to continue support for these events. To change the default ifs share name, click the "Isilion admin share name" link on the top right corner of the page. • **Volume** - select this option to audit a single volume. Then enter the volume name (<*VolumeName*>) or click the browse button to locate and select the volume to be audited. **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. **NOTE: Isilon file server auditing**: Volume auditing is not supported and should not be used. Once you have entered the audit path to be audited, use the **Add** button to add it to the selection list.
...	Click the browse button to locate and select the file, folder or volume to be audited. If you select an invalid file, folder or volume a red flashing icon appears explaining that your selection is invalid. **NOTE:** This button is not available when **All Volumes** is selected as the audit path.
Add	Use the **Add** button 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 for the 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.

Table 1. EMC Auditing wizard

Events tab: Use the Events tab to select vital file and/or folder events. **NOTE:** The process for capturing ACL events is extremely slow. See Performance Considerations for more details on the process used to capture ACL 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 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/Folder Inclusion and Exclusion Examples for more file mask examples. You can also enter the name of an individual subfolder or file that is to be included. However, if you enter the name of a subfolder, you will only receive events for operations performed against the specified subfolder. You will NOT receive events for operations performed against any child objects under the specified subfolder. Once you have specified the subfolders or files to be included, click **Add** to add it to the Inclusions list.
Inclusions list	The list across the bottom of this page contains the subfolders and files selected for auditing. Use the buttons to the right of the text box to add and remove entries.
Add	Use **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.	

Table 1. EMC 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 that is to be excluded from auditing. **IMPORTANT:** If you enter the name of a subfolder or file that is outside of the audited path, Change Auditor will not exclude it from auditing. Once you have selected a subfolder or file to be excluded, select the appropriate **Add** button to add it to the Exclusions list.
Exclusions list	The list across the bottom of this page contains the folders, files and masks that are to be excluded from auditing. Use the buttons to the right of the text box to add and remove entries.
Add	Use one of the following **Add** commands to move the entry in the text box to the Exclusions list: • **Add | Folder** - use this option to exclude activity against files/subfolders in any folders that match the exclusion string. • **Add | File** - use this option to exclude activity against any files that match the exclusion string.
Remove	Select an entry in the Exclusions list and click the **Remove** button to remove it.
Select Change Auditor agents page: Use this page to select the agents that are to receive the events captured on the selected EMC file server (CIFS). **NOTE:** You may improve performance by assigning an EMC Auditing template to more than one Change Auditor Agent. When multiple agents are assigned to the same EMC Auditing template, events will be load balanced between these agents. However, the downside is that the 'where' field for EMC events may contain any one of the agents being monitored by this single auditing template. In addition, if EMC event logging is enabled in Change Auditor, events will be written on multiple agent servers.	
Add	Click **Add** to assign one or more agents to the EMC Auditing template. Selecting this button displays the Eligible Change Auditor Agents dialog. From this dialog, select one or more agents and then click **OK**.
Remove	Click **Remove** to remove the selected agent from the list.

Table 1. EMC Auditing wizard

Set Credentials	Click the **Set Credentials** button to enter the credentials to be used to access the selected EMC Control Station: • **Control Station** - enter the IP address of the EMC Control Station. • **User** - enter the user name of an account with Administrative rights (rights to create or modify the cepp.conf file) on the selected EMC Control Station. • **Password** - enter the password associated with the user name entered above. • **Data Mover** - select the data mover that hosts the EMC file server (CIFS) specified on the first page of the wizard. Click the **Test** button to validate the credentials entered. Once the credentials are validated, click **OK** to set the credentials as entered and close the dialog. **NOTE:** There is no need to enter the EMC Control Station credentials when configuring auditing on an Isilon server.
Change Auditor Agent list	The list across the bottom of the page lists the Change Auditor agents selected to capture events from the selected EMC file server (CIFS).
CEPP.CONF file page: If you have changed or added agents to your template, use this page to review the changes you are proposing to make to the cepp.conf file. This page displays the current and proposed cepp.conf files. In addition to viewing the current and proposed cepp.conf files, you can optionally make changes to the proposed cepp.conf file or deploy the proposed cepp.conf file on the selected EMC Control Station. **NOTE: Isilon file server auditing:** This information is not required; click **Finish** to create the EMC Auditing template.	
Update File	Click **Update File** to deploy the proposed configuration file on the EMC Control Station.
Check Status	Click **Check Status** to run the following command to check the status of the cepp service: server_cepp <*Data Mover Name*> -pool -info **NOTE:** The information provided in the status check window can be used for troubleshooting. For example, a red Connection Disconnected entry could indicate one of the following scenarios: • CAVA service is not connected • Change Auditor agent is offline • Shared EMC Connector service is not running
Audit File	Click the **Audit File** button to enable or disable the auditing of the cepp.conf file for changes made by other third-party applications. **NOTE:** When this configuration file is being audited, an event is generated whenever another application modifies the configuration file. Modifications made to this configuration file by another application may prevent Change Auditor from capturing EMC events. Clicking this button displays the Configure cepp.conf Auditing dialog. To enable the auditing of this file, select the **Enable Auditing** check box and select a Change Auditor agent that is to poll for changes. Click **OK** to save your selections and close the dialog.
Current cepp.conf File	Displays the contents of the current cepp.conf file on the selected EMC Control Station.
Proposed cepp.conf File	Displays the proposed content of the cepp.conf file based on the selections made in the EMC Auditing wizard. **NOTE:** You can manually edit the contents of the proposed cepp.conf file from this page.

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** to display the Agent Configuration page.
4. Click **Configurations**.
5. On the Configuration Setup dialog, select an agent configuration from the left pane (i.e., the configuration that is being used by the Change Auditor agents assigned to receive EMC® events).
6. Open the File System tab and modify the settings to define how to process duplicate file system events 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 agent(s) assigned to the EMC Auditing template (**Auditing** appears in the **EMC** 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.

EMC event logging

In addition to real-time event auditing, you can enable event logging to capture EMC 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 EMC event log. See the Change Auditor for EMC 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 **EMC Events**.

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

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

4

EMC Searches/Reports

- Introduction
- Create custom EMC searches

Introduction

You can create custom search definitions to search for file and/or folder changes to a specific EMC 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 EMC 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 EMC searches

The following scenarios explain how to use the What tab to create custom EMC 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 EMC 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 enables the Search Properties tabs across the bottom of the Searches page.
4. On the Info tab, enter a name and description for the search.
5. Open the What tab, expand **Add** and select **Subsystem | File System**.
6. On the Add File System Path dialog, select **All File System Paths**.
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 EMC events and display the results in a new search results page.

To search for events performed against a specific EMC 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** at the top of the Searches page.

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

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

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

6 On the Add File System Path dialog, select 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 EMC path to be searched.

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

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

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

NOTE: If the scope of your search is **This Object**, you can use the * wildcard character to specify the EMC 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 EMC 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 EMC events in the selected path and display the results in a new search results page.

To search for a specific EMC 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** at the top of the Searches page.

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

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

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

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

- 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 Change Auditor agent collecting the EMC events.

- Hardware considerations
- Load balancing

Hardware considerations

To improve agent performance, you can:

- Upgrade the link between the EMC file server and the Change Auditor 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 System overview for more information.

Load balancing

You can also improve performance by assigning an EMC Auditing template to more than one agent. When multiple agents are assigned to the same EMC Auditing template, events will be load balanced and events will be sent to each agent round-robin style.

TIP: Quest recommends that you specify no more than two agents; however, you can specify more than two agents if you find the need. The downside to assigning multiple agents to the same EMC Auditing template is that the 'where' field for EMC events may contain any one of these agents. In addition, if EMC event logging is enabled in Change Auditor, events will be written on multiple agent servers.

Configuring audit scope

Audit only volumes, extensions and operations that are vital for your environment.

NOTE: Configuring the auditing scope to audit only critical files/folders is recommended because this filtering controls the traffic between the coordinator and agent. However, changes to the auditing scope as described below will have no impact on the traffic between EMC and the agents.

Use the EMC Auditing template to specify the auditing scope for EMC events. For example, using the EMC 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*>\<*FolderName*>\<*FileName.ext*>
    - To specify a folder, enter: <*ShareName*>\<*FolderName*>
    - To specify a volume, enter: <*VolumeName*>
- Decrease the number of file extensions being audited
  - Use the Inclusions tab to specify individual subfolders or files to be included for auditing.
  - 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/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

EMC Events

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

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

Folder events

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

7

File/Folder Inclusion and Exclusion Examples

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

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 1. Inclusion examples

What to include 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 1. Inclusion examples

What to include 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>)

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

Table 2. 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 2. 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>)

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. See examples below.

Table 3. 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

Table 3. Exclusion examples: Audit Path = Volume

What to exclude:	Exclusion syntax/examples:
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
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\DOCS\Testing.doc Vol0\HOME\USERS\TEMP\DOCS\BetaDoc.pdf Vol0\SHARE2\USERS\DOCS\Test1.docx Vol0\SHARE2\PUBLIC\MYDOCS\OldDocPlan

Table 3. Exclusion examples: Audit Path = Volume

What to exclude:	Exclusion syntax/examples:
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

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. See the following examples.

Table 4. 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
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

Table 4. Exclusion examples: Audit Path = All Volumes

What to exclude:	Exclusion syntax/examples:
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

8

EMC Isilon Auditing

EMC Isilon file server auditing is supported; however, automatic Isilon auditing configuration is not supported. This section discusses the manual configuration required to capture events from an Isilon file server.

Configuration Notes

- On the agent intended to audit the Isilon server, install CEE. You may need to configure the firewall setting on your server before the CEE application can receive events from an Isilon server.
- Change Auditor does not support automatic Isilon auditing configuration. To enable Isilon file server auditing, use the Isilon management web site UI and command line interface.

  See EMC OneFS Web Administration Guide (http://bit.ly/onefs-web-administration-guide-7-1) and EMC OneFS CLI Administration Guide (http://bit.ly/onefs-cli-administration-guide-7-1) for more information.

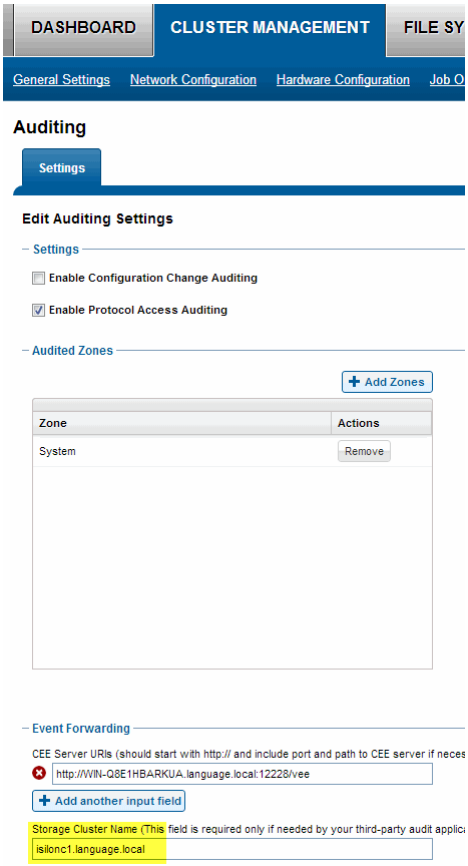
  NOTE: An EMC account is required to access these EMC administration guides.

- When asked for the URI for the CEE server, use the following format:

  'http://<*FQDN of CA agent/CEE server*>:12228/vee'

- To configure Change Auditor for EMC to audit an Isilon server, use the EMC Auditing wizard. Isilon servers are not listed in the **EMC File Server (CIFS)** drop-down, but can be manually entered:

  Make sure that the server name specified is the one configured in the Isilon auditing setting:



- 'Volume' auditing is not supported on Isilon servers and should not be used.
- When specifying file and folder paths to be audited, the Isilon's shared directory path should be used. You can find it in Isilon management web site UI by going to Protocols – Windows Sharing (SMB) – SMB Shares.

  For example: To audit \\IsilonName\Storage\TestFolder folder, you need to specify ifs\data\TestFolder in the Audit Path field of the template in Change Auditor. Ensure that the backslash (\) is used in the path in Change Auditor template.
- Owner and permission events are supported, but events captured contain only 'to' values and no 'from' values. To capture permission changes on Isilon, the Change Auditor agent account (typically the Local System account which translates to the agent computer account) should have Read permissions on the IFS share (or its equivalent). This can be accomplished by adding a computer account to a group and granting Read access to the group.

  Individual computer accounts can also be added using ISI command line on the Isilon itself.

  For example: isi smb shares permission create ifs --sid COMPUTER_ACCOUNT_SID --permission-type allow --permission read

  In addition, agent computer accounts require Read access to all the files\folders to be audited (via Windows security). In the case where users have modified the default inherited security on their folders/files, Change Auditor will be unable to query those items.There is no need to enter information on the Logon Credentials dialog when configuring auditing on an Isilon server.
- To audit the "File contents written" operations, you must audit "Close" operations on Isilon. To audit close operations, use isi zone zones modify command in the command line interface (CLI).

  For example:

  - To audit a successful close operation for the 'System' zone run the following command:
    isi zone zones modify system --add-audit-success close.

- To review all currently audited operations for the System zone, use the following command:
  isi zone zones view system

9

EMC Unity Auditing

EMC Unity NAS server auditing is supported; however, automatic unity auditing configuration is not. This section discusses the manual configuration required to capture events from a Unity NAS server.

Configuration Notes

- On the agent intended to audit the Unity NAS server, install CEE. You may need to configure the firewall setting on your server before the CEE application can receive events from a Unity server.
- Change Auditor does not support automatic Unity auditing configuration. See the EMC Unity documentation for configuring host for more information.

  To enable auditing, you must configure CEE using EMC Unisphere:

  - Select **STORAGE | File | NAS Servers**. Open the server properties and select **Event Publishing**. Select to **Enabling Common Event Publishing.** Add the CEPA Server where the CEE is installed, select **All Events**, and save the settings.
  - Select **File System** you want to audit and choose the **Advanced** tab. Under the **Events Notifications,** select **Enable SMB Events publishing**.
- When you create the EMC auditing template to audit a Unity NAS server, you need to enter the NAS servers as they are not listed in the EMC File Server (CIFS) drop-down option. Ensure that you specify the server configured in the Unity auditing setting. For details on creating a template, see EMC auditing templates.

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.