Quest® Change Auditor 7.1
Web Client User Guide

Legend

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

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

Change Auditor Web Client User Guide
Updated - June 2020
Software Version - 7.1

Contents

Install Change Auditor Web Client

- Introduction
- Deployment requirements
- Install web client
- Troubleshooting tips

Introduction

The web client is installed on the Internet Information Services (IIS) web server which allows access to Change Auditor data using a standard or mobile browser. Similar to the Windows client, you can use the web client to run searches and reports on the data collected by Change Auditor, create custom search queries, and perform administration tasks to manage Change Auditor. In addition, you can display the search results in a timeline and create custom shared overviews which can then be shared with other users interested in viewing the selected Change Auditor data.

This guide has been prepared to assist you in becoming familiar with the Change Auditor web client. This document provides a description of the main components in the web client when started using a standard browser and procedures for the web client functions. It also includes a comparison of the Windows client and the web client.

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.

Install web client

> **i** | **NOTE:** The web client requires that IIS is installed on an application server. The following procedure assumes that IIS is already installed.
>
> For more information about installing the default configuration of IIS, see the Microsoft website, such as: http://technet.microsoft.com/en-us/library/ee692294(WS.10).aspx.

Install the web client:

1 On the IIS web server, insert the Change Auditor DVD or if you downloaded the product from the Quest web site, run the **autorun.exe** file to start the Quest Change Auditor autorun.

2 On the Install page, click **Install** for the **Install Change Auditor Web Client** option to start the Change Auditor Web Client Setup wizard.

3 On the Welcome screen, click **Next**.

4   On the Select Installation Folder screen, click **Next** to use the default location. Use **Browse** to specify a different location, then click **Next**.

5   From the Internet Information Services screen, you can enter a website name for the web client and change the default port for the website.

> **i** | **IMPORTANT:** Select a unique port for the website to avoid conflicts with other IIS applications (for example, SharePoint uses the default port 80; therefore, the IIS website for the web client must use a different port). If a conflicting port is specified, attempting to start the web client displays either an 'HTTP 404 Not Found' or 'Page cannot be displayed' error.

6   On the Coordinator screen, select the coordinator for which data is to be made available through the web client. The drop-down menu displays a list of coordinators available.

> **i** | **NOTE:** If the web client is not a member of the domain and the coordinator cannot be detected (that is, it is not displayed or listed in the drop-down list), enter the IP address or server domain name of the coordinator to use.

Click **Install**.

7   Click **Finish** to exit the wizard.

8   After the web client is successfully installed, click **Close**.

Add accounts to Change Auditor security groups:

Once the web client is installed, you must add all the user accounts who will be using it to one of the following security groups depending on the level of access required.

1   Users requiring full access to the web client must be added to the ChangeAuditor Administrators - *<InstallationName>* Group.

2   Users who require access to perform all tasks but not administrative functions should be added to the ChangeAuditor Operators - *<InstallationName>* Group. Users added to this group can view Shared Overviews; but they will not have access to the Shared Overview Administration page.

3   Users who only need access to view Shared Overviews should be added to the ChangeAuditor Web Shared Overview Users - *<InstallationName>* Group.

Start the web client:

1   Open your web browser and enter the URL of the web application server.

http://*<Web Server Host Name>*/ChangeAuditor

> **i** | **NOTE:** If you specified a different default port (other than 80) on the Internet Information Services screen of the setup wizard, you must also enter the default port specified:
> http://*<Web Server Host Name>*:*<Port>*/ChangeAuditor

2   When the web client is started, log on by entering the user name (*<Domain>\<UserName>*) and password of an authorized Active Directory account.

> **i** | **NOTE:** Selecting the **Remember Me** check box will retain your *<Domain>\<UserName>* on subsequent sessions.

3   Click **Log In**.

The web client opens, displaying the Overview page.

> **i** | **NOTE: Upgrading the web client**
> After you have upgraded the web client, you may need to force your browser to reload the Change Auditor web pages from the web server (CTRL-F5 for IE, Chrome ,or Firefox) to ensure you are seeing the most up-to-date changes made to style components within the web client (for example, icons, text or images). See the documentation for your browser for further details.

Troubleshooting tips

If you cannot successfully log in to the web client, verify the following:

- Ensure that the correct port number is specified in the connection settings of the web.config file. The port number is specified after the colon in the following statement in the <appSettings> section:

  `<add key="Coordinator" value="<DNS name or IP address>:<port>"/>`

  > **i** | **NOTE:** If you are using a dynamic port assignment, the coordinator may be assigned a new port whenever it is restarted. Therefore, every time the coordinator is restarted you must check/update the port number in the web.config file to ensure the coordinator's new SCP port is specified.

- If the coordinator host cannot be resolved by DNS, you must specify the IP address instead of the DNS name in the connection settings of the web.config file. The IP address is specified before the colon in the following statement in the <appSettings> section:

  `<add key="Coordinator" value="<IP address>:<port>"/>`

- If the coordinator is running under a service account (not the LocalSystem account), you will get an authentication error when logging in to the web client. If this happens, change the DNS name specified in the web.config file to the appropriate IP address of the server hosting the coordinator.

Web Client Overview

- Introduction
- Open the web client
- Web client components
- Change Auditor settings
- Customize table content
- Filter data
- Directory object picker

Introduction

The web client enables you to perform administrative tasks, search for configuration changes and view Change Auditor data using a web browser rather than the Windows client.

> **i** | **NOTE:** The web client's appearance is different based on whether you have started it using a standard browser or a mobile browser. The procedures in this guide illustrate the standard browser version of the web client.

Open the web client

To open the web client:

1   Open your web browser and enter the URL of the web application server.

   http://<*Web Server Host Name*>/ChangeAuditor

   > **i** | **NOTE:** If you specified a different default port (other than 80) on the Internet Information Services screen of the setup wizard, you must also enter the default port specified:
   > http://<*Web Server Host Name*>:<*Port*>/ChangeAuditor

2   When the web client is opened, log on by entering the user name (<*Domain*>\<*UserName*>) and password of an authorized Active Directory account.

   > **i** | **NOTE:** Selecting the **Remember Me** check box retains your <*Domain*>\<*UserName*> on subsequent sessions.

   Depending on how your system has been configured, you can select the option to disconnect the client from the coordinator after 30 minutes of inactivity.

3   Click **Log In**.

   The web client opens and displays the Start page.

Start Page

From the Start page, you can view and access relevant information regarding Change Auditor including news and updates, support, and knowledge base content, online documentation, links to the latest releases, and essential contact links.

If you do not want to see this page each time that you open the web client, then clear the **Display this page each time I log in** option. One this option has been cleared, the next time you log in you will be directed automatically to the Overview page. However, we suggest you keep the Start page active as it contains the most up-to-date access to the supporting information you may require.

Web client components

The Change Auditor web client consists of the following components allowing you to navigate through the client and define the content to be displayed:

- Heading bar
- Main web pages

Heading bar

The heading bar, at the top of each web page, contains links to the Quest Software website, web client settings, and general information about the web client:

- Click the Quest logo in the left corner to launch the IT & System Management page on Quest Software's web site.
- Click the Change Auditor logo to start the Change Auditor product page on Quest Software's website.
- Click the <*Username*> in the upper right corner and select **Sign Out** to disconnect from the web client.
- Click the gear icon to view or modify the web client settings. See Change Auditor settings for more information regarding these settings.
- Click the information icon to display the About Change Auditor Web Client dialog which displays general release information about Change Auditor, including version, copyright, patent, licensing, legal notices, and contact information.

Main web pages

The Change Auditor web client consists of the following main web pages:

Table 1. Main web pages

Page	Description
Start Page	Provides up-to-date product information.
Overview Page	Provides a rotating view of predefined overview panes and allows you to customize your own view of Change Auditor activity.
Shared Overviews Administration Page	Allows you to define custom views which can be shared with other users.
Searches Page	Allows you to run searches and create custom searches to retrieve events captured in the Change Auditor database.
Administration Tasks Page	Allows you to perform a variety of administration tasks.

To open one of these pages, click the arrow on the upper left of each page, directly beneath the Quest logo, to expand a list of the main web pages.

> **i** | **NOTE:** You can also click a page's icon to open the page without expanding the menu.

When a search is run, an extra page is added:

- Search Results Page - displays details about the events retrieved from the Change Auditor database.

When a hot spot or hypertext link is selected within an overview pane, an extra page is added:

- Overview drilldowns page - displays more details based on the hot spot or hypertext link selected in an overview pane. This additional page could contain a Search Results page, Agent Statistics page, or Coordinator Statistics page.

Change Auditor settings

The web client has its own settings which can be used to control the contents to be displayed.

> **i** | **NOTE:** Unlike the Change Auditor Windows client where these settings can be defined for each individual search, the settings on the web client are global, and control the display of ALL searches.

To change the web client settings:

1. Click the gear icon at the top of the web client page.
2. On the Client Settings dialog, review and modify the settings as described below:

Table 2. Client settings

Setting	Description	Default
Searches tab		
Max # of search columns	This setting defines the maximum number of columns that can be displayed on the Search Results tab in the web client. Valid values are: 1 - 150.	30
Show SQL Tab	Select this check box to add the SQL tab to the Search Properties on the Searches page. This tab displays the SQL script used to create the selected search definition.	Not selected/ displayed
Show XML Tab	Select this check box to add the XML tab to the Search Properties on the Searches page. This tab displays the XML representation of the search criteria.	Not selected/ displayed
Slideshow Options tab		
Rotate Views Every	Specifies the rotation interval for the panes displayed in slideshow mode on the Overview page.	1 minute
Client Connectivity	Use the Disconnect client after 30 minutes of inactivity option to disconnect from the client after 30 minutes of inactivity. If this option is not checked, the connection to the coordinator remains open.	Not selected

3. Click **Save** to save your selections and close the dialog.

   Click **Cancel** to close the dialog without saving your selections.

Customize table content

The contents of the various data grids displayed in the web client can be sorted, rearranged, and grouped.

Sort data

An arrow in the column heading identifies the sort criteria and order, ascending or descending, being used to display information.

To change the sort criteria:

1   Click the column heading to be used for the sort criteria.

2   The sort order is in ascending order, but can be changed to descending order by clicking the heading a second time.

3   To specify a secondary sort order, click the heading of the column to use for the secondary sort order.

4   To remove the sort order from a column, click the column heading until the arrow disappears.

¡ | **NOTE:** Selecting the **F5** key to refresh your screen removes any sort criteria that you have applied.

Resize columns

Columns can also be resized within a data grid.

To resize a column:

1   Place your cursor on the boundary between column headings (the cursor changes to a double-arrow).

   ¡ | **NOTE:** For primary columns (the columns shared by all data grid items), the boundary is located to the right of the column's filter button. For secondary columns (any item specific columns), the boundary is located to the left of the column's filter button.

2   Click and hold the left mouse button dragging the column boundary to the desired size.

Add or remove columns

Change Auditor displays a default set of columns for the different pages displayed. However, a few pages allow you to display more data or hide a particular column.

To add or remove columns:

1   Click **Columns** located above the column headings.

   A drop-down list is displayed which shows the data (columns) available for display.

2   From this list, select the columns to display and clear the columns you do not want displayed.

3   Once you have selected all the columns to display, click outside of the drop-down list to close it.

   ¡ | **NOTE:** For each individual search, you can select the data to be retrieved and displayed in the client using the Layout search properties tab. From this tab you can also define column order, sort criteria and order, groupings and the format to be used for displaying the retrieved data.

Expand properties button (right arrow)

The expand properties button (right arrow) is displayed throughout the web client, and is located to the left of any container that can be expanded to show more items or collapsed to hide unneeded items. When the arrow is displayed pointing to the lower-right it is expanded, and when the arrow is pointing to the center-right it is collapsed.

Additional expand properties buttons that appear within an expanded container will be hidden if the original container is collapsed. When the original container is re-expanded, all expand properties buttons within the original will appear as they were last set.

Filter data

Traditional search capabilities provide the first phase of drilling down on details you may be seeking, but locating individual events typically requires more granular search capabilities and additional steps. Change Auditor provides advanced filtering options to modify the results of a search without changing the original search. With this capability, filtering can be performed on one or more columns of a result, ultimately reducing the need to build the same search multiple times with minor customizations.

To filter data:

Throughout the web client, you will see a filter icon in the right-hand corner of column headings. This icon provides data filtering options which allow you to filter and sort the data displayed.

1   Click one of the filter icons to expand the filter options for that column.

2   By default, the web client uses the 'Is equal to' expression to filter the data. However, clicking the current expression displays a list of available expressions.

3   Depending on the data being filtered, one of the following controls appears:

   - Select Value field — click **Select Value** to display a list of options and select a value from this list.

   - Text box (blank box) — enter the word or string of characters to use to filter the data displayed.

   i | **NOTE:** The filtering feature is case sensitive.

4   Click **Filter** to filter the data according to your criteria.

5   To remove the filtering from a column, click the filter icon to expand the filtering options and click **Clear**.

i | **NOTE:** Selecting the **F5** key to refresh your screen removes any filtering that you have applied.

Directory object picker

Throughout the web client, you will encounter the directory object picker which allows you to locate and select a directory object from your environment. This object picker is displayed in either a stand-alone dialog (for example, Select Active Directory Objects dialog) or as a page in a wizard and consists of the following tabbed pages:

•   **Browse** - use the Browse page to select a directory object from a hierarchical view of your environment

•   **Search** - use the Search page to search your environment to locate and select a directory object

To browse for a directory object:

1   Click **Browse**.

2   In the **Forest** field, select the forest that contains the required directory objects.

>   **NOTE:** The Forest field is available in directory object picker in the following areas:
>   - Group membership expansion and SMTP configuration
>   - Purge and archive jobs
>   - Active Directory, AD Query, ADAM (AD LDS), Exchange, and Group Policy searches
>   - Active Directory auditing and protection wizard
>   - File System protection wizard

3   In the **Find** field, either enter or use the drop-down menu to select the type of directory objects to be displayed.

You can enter multiple classes, separated by either a comma or semi-colon. Note that when you type in an entry, you must use the **Enter** key to display the objects.

>   **NOTE:** Most of the time, this field will be automatically filled in with the appropriate entry. Thus, when this field is grayed out, this is a read-only field which cannot be changed.

4   In the explorer view (left pane), single-click on the expand properties button (right arrow) to the left of the container or double-click a container to expand the view to display subordinate objects.

Select a container in this pane to populate the object list (right pane) with the objects that belong to the selected container.

5   In the object list, click an object to select it and then click **Add** to add it to the selected objects list at the bottom of the dialog.

>   **NOTE:** The Selected Objects list is used for both the Browse and Search pages and will contain the objects selected from either of these pages.

6   Once you have added objects to this list, click **OK** to save your selection and close the dialog. Or if the directory object picker is part of a wizard, click **Next** to save your selection and continue.

To search your environment to locate a directory object:

1   Click **Search** and use the controls at the top of the page to search your environment to locate the desired objects.

2   In the **Find** field, either enter or use the drop-down menu to select the type of directory object to locate.

You can enter multiple classes, separated by either a comma or semicolon. When you type in an entry, you must click **Search** to display the objects.

>   **NOTE:** Most of the time, this field will be automatically filled in with the appropriate entry. Thus, when this field is grayed out, this is a read-only field which cannot be changed.

3   In the **Name** field, specify a search expression to use to search Active Directory to locate a particular object. Usually, this field contains an asterisk (*) indicating to search for all objects of the type specified in the **Find** field.

The **ANR** check box is checked by default indicating that Ambiguous Name Resolution (ANR) is the search algorithm used, which allows you to enter limited input (partial data) to find multiple objects in your network.

When the **ANR** check box is checked, use one of the following methods to enter your search expression:

- Enter a partial string to return exact matches or a list of possible matches. For example, entering 'Admin' will return objects that contain the names 'Admin', 'Admins', 'Administrator', 'Administrators', etc.

- Enter a string preceded by the equal sign (=Admins) to return only exact matches. For example, entering '=Admin' returns only those objects containing the name 'Admin'.

By default, ANR searches the following attribute fields in Active Directory:

- First Name (GivenName)

- Last Name (Surname)

- Display Name (displayName)

- LegacyExchangeDN

- msExchMailNickname

- Relative Discontinued Name of the object (RDN)

- Office (physicalDeliveryOfficeName)

- Email address (proxyAddress)

- Security Account Manager account (sAMAccountName)

When the **ANR** check box is cleared, the search expression entered is used to search only the Display Name of directory objects to locate a particular object.

To use this search mechanism, enter a string of characters and the wildcard (*) character as described below.

- n* returns objects that start with the letter 'n'

- *n returns objects that end in the letter 'n'

- *n* returns objects that contain the letter 'n' within their Display Name.

4   After entering a search expression, click **Search** to initiate the search and return the results of the search.

5   The object list displays the objects found as a result of your search. To select an object, click the object to select it and then click **Add** to add it to the Selected Objects list.

> **i** | **NOTE:** The Selected Objects list is used for both the Browse and Search pages and will contain the objects selected from either of these pages.

6   Once you have added objects to this list, click **OK** to save your selection and close the dialog. Or if the directory object picker is part of a wizard, click **Next** to save your selection and continue.

Overview Page

Introduction

The Overview provides access to valuable information about Change Auditor and the events being captured. From here, you can view Change Auditor data in one of two modes:

- Slideshow mode which rotates through a set of predefined overview panes.
- Custom Views mode which allows you to create a custom view to display only the overview panes you are interested in seeing.

i | **NOTE:** On a mobile browser, the Overview page displays the overview panes defined on the user's custom view page. The slideshow and custom view modes are not available in the mobile browser version.

Slideshow mode

The slideshow mode is the default mode when the Overview page is initially displayed. In this mode, predefined overview panes are displayed, six to a screen, rotated based on the interval specified on the Slideshow Options page of the Client Settings dialog.

Use the tool bar buttons across the top of the Overview page to scroll through the overviews and to switch to the custom view mode:

Table 3. Slideshow mode: Tool bar buttons

Tool bar button	Description
Custom Views	Select to switch to the custom views mode where you can select the widgets (i.e., queries) to be displayed.
Previous	Use to redisplay the previous six overview panes in the slideshow.
Pause | Play	Select **Pause** to stop the rotation and remain on the current page. Use **Play** to resume the rotation of the overview panes.
Next	Use to display the next six overview panes in the slideshow.

Custom Views mode

Using the custom views mode you can specify the overview panes to be displayed as well as specify how and what is to be displayed in each of the selected overview panes. By default, the following overview panes are included in the initial custom view:

- Agent Activity
- Agent Status: Enterprise
- Count of Events by Severity

Use the tool bar buttons across the top of the Overview page to define the widgets (overview panes) to be included, refresh the client and to switch over to the slideshow mode:

Table 4. Custom views mode: Tool bar buttons

Tool bar button	Description
Slideshow	Select to switch to the slideshow mode and rotate through all of the default overview panes.
Widgets	Use to display the widgets list, from which you can select the queries to be included as overview panes in your custom view.
Refresh	Use to refresh the screen to display the selected overview panes.
Expand All	Use to expand all collapsed overview panes in the current view.
Collapse All	Use to collapse all of the overview panes in the current view.

Overviews/widgets

The following views have been pre-built and are available for display from the Overview page. When in the slideshow mode, the client rotates through each of these queries, displaying six overview panes at a time. In the custom views mode, selecting the **Widgets** button allows you to select which of these queries are to be included for the current user.

- Accounts Overview (Locked/Disabled/Enabled)
- Agent Activity
- Agent Status: Enterprise
- Agent Status: Other
- Agent Status: Workstation
- Agent Status: *<Domain>*
- Alert History
- Alert History Counts by Query
- Coordinator Status: Enterprise
- Coordinator Status: *<Domain>*
- Count of Events by Event Class
- Count of Events by Facility
- Count of Events by File System Permission Changes
- Count of Events by Location
- Count of Events by Result
- Count of Events by Severity

- Count of Events by Subsystem

- File Access Rights

- File Ownership

- Recent Event Activity

ℹ️ | **NOTE:** Additionally, you can create a custom widget from any search by using the **Show as Widget** check box located on the searches' Info tab. See Searches Page for more information on adding a search query to the widget list.

Create a custom view

To create a custom view:

1 From the Overview page, click **Custom Views**.

2 Click **Widgets** to display a list of the widgets available.

3 Select a widget from the list:

- To add the pane into the upper left pane of the page, click the widget to be added.

- To add the pane to a specific pane on the page, drag 'n drop the widget into the desired pane.

ℹ️ | **NOTE:** You can use the links in the Filter By pane to filter the widget list. For example, to see only the widgets that pertain to agent status, select the **Agent Status** link. To redisplay all of the widgets available, select the **All Widgets** link at the top of the Widgets pane.

Repeat this step to add additional widgets, up to a maximum of nine, to the Overview page.

4 Once you have selected the widgets to be included, use the **Close** button (X) in the upper right corner to collapse the Widgets and Filter By panes to view the newly created Overview page. You can also click **Widgets** to collapse the Widgets pane.

5 To rearrange the overview panes on the page, click in the heading of a pane and drag it to the new location on the page.

6 To change the content or format of an individual overview pane, click the edit button in the upper right corner of the pane.

Selecting this button displays parameters that can be used to customize the individual pane.

Once you have changed a parameter, click **OK** to save your selection and close the parameter pane.

Collapse, expand or remove a widget

To collapse, expand or remove a widget:

1 Select one of the following tool bar buttons in the upper right corner of a widget:

- Use the up arrow to collapse the widget and just display the heading. You can use the **Collapse All** button in the page tool bar to collapse all the widgets in the current view.

- Use down arrow to expand a collapsed widget to display its contents. You can also use the **Expand All** button in the page tool bar to expand all collapsed widgets in the current view.

- Use the X to remove the widget from the current view.

Overview drilldowns page

Many of the overview panes contain hot spots or hypertext links which when selected open a new page under the Overview Drilldowns tab. The following table explains the hot spots/hypertext links available on the different overview panes and the page that is displayed when selected.

Table 5. Overview panes: Hot spots/hypertext links

Overview pane	Hot spot/Hypertext link	Page displayed
Accounts Overview	Bar Graph: The bars in the graph are hot spot links.	Search Results page containing the events associated with the selected bar.
Agent Activity	Audit Events: The value listed for each agent is a hypertext link.	Search Results page containing the events generated by the selected agent.
Agent Status	Active Agent graphic is a hot spot link.	Agent Statistics page displaying agent details. **NOTE:** Events Today and Events Total entries are hypertext links to a corresponding Search Results page.
Coordinator Status	Active Coordinator graphic is a hot spot link.	Coordinator Statistics page displaying coordinator details. **NOTE:** Events Today entries are hypertext links to a corresponding Search Results page.
Count of Events by Event Class	Audit Events: The value listed for each event class is a hypertext link. Bar Graph: The bars and numeric values in the graph are hot spot links.	Search Results page containing the events generated within the selected event class.
Count of Events by Facility	Audit Events: The value listed for each facility is a hypertext link. Bar Graph: The bars and numeric values in the graph are hot spot links.	Search Results page containing the events generated within the selected facility.
Count of Events by File System Permission Changes	Audit Events: The value listed for each agent is a hypertext link. Bar Graph: The bars and numeric values in the graph are hot spot links.	Search Results page containing the file system permission change events captured in the last 7 days.
Count of Events by Location	Audit Events: The value listed for each location is a hypertext link.	Search Results page containing the events captured at the selected location.
Count of Events by Result	Bar Graph: The bars in the graph are hot spot links.	Search Results page containing the events associated with the selected result bar.
Count of Events by Severity	Bar Graph: The bars in the graph are hot spot links.	Search Results page containing the events associated with the selected severity bar.
Count of Events by Subsystem	Audit Events: The value listed for each subsystem is a hypertext link. Bar Graph: The bars and numeric values in the graph are hot spot links.	Search Results page containing the events generated within the selected subsystem.
File Access Rights	Audit Events: The value listed for each event class is a hypertext link.	Search Results page containing the events generated within the selected event class.

Table 5. Overview panes: Hot spots/hypertext links

Overview pane	Hot spot/Hypertext link	Page displayed
File Ownership	Audit Events: The value listed for each event class is a hypertext link.	Search Results page containing the events generated within the selected event class.
Recent Event Activity	Bar Graph: The bars in the graph are hot spot links.	Search Results page containing the events associated with the selected bar.

Shared Overviews Administration Page

* Introduction
* Manage shared overviews

Introduction

The Shared Overviews Administration page allows you to create custom overviews and share these overviews with other users who have expressed interest in viewing the selected data. Click the **Shared Overviews** link in the expanded left pane to display this page.

> **i** | **NOTE:** The Shared Overviews Administration page is only available to users who have the 'View Web Overview Administration' authorization. By default, users in the ChangeAuditor Administrators security group have this authorization.
>
> Adding users to the ChangeAuditor Web Shared Overview Users security group will allow them to view Shared Overviews, while restricting them to only what has been shared.
>
> See the Application User Interface Authorization page chapter for more information on granting permissions to users.

> **i** | **NOTE:** The Shared Overviews Administration page is not available in the mobile browser version.

This page contains a list of shared overviews previously defined. Initially, this page is empty. Click **Add** to add a new overview to the list.

Use the tool bar buttons across the top of the Shared Overviews Administration page to create and manage shared overviews:

Table 6. Shared Overviews Administration page: Tool bar buttons

Tool bar button	Description
Add	Use to create a new shared overview.
Email	Use to email a link to the overview selected in the overview list.
View	Use to open a new tabbed page to view the queries contained in the selected overview. This is a read-only view. **NOTE:** You can also double-click an overview in the list to view the queries contained in the selected overview.
Edit	Use to make changes to the overview selected in the shared overview list.
Copy	Use to create a copy of the overview selected in the shared overview list.
Delete	Use to delete the overview selected in the shared overview list.

In addition to the Shared Overviews Administration page that lists the shared overviews available, there is also an edit page, which allows you to add a shared overview or edit an existing shared overview. The edit page displays the name of the shared overview and contains the following tool bar buttons:

Table 7. Shared Overviews Administration edit page: Tool bar buttons

Tool bar button	Description
Widgets	Use to display the widgets list, from which you can select the queries to be included as overview panes in the shared overview.
Rename	Use to rename the shared overview. Selecting this button displays the Rename dialog allowing you to enter the new name for the overview.
Email	Use to email a link to the selected overview.
Expand All	Use to expand all collapsed overview panes in the current view.
Collapse All	Use to collapse all of the overview panes in the current view.

Manage shared overviews

To create a new shared overview:

1   From the Shared Overviews Administration page, click **Add**.

2   On the New Shared Overview dialog, enter a unique name for the overview and click **Save**.

3   An edit page appears allowing you to define the contents of the overview.

By default, the Agent Activity, Agent Status: Enterprise, and Count of Events by Severity overview panes are displayed.

4   To add an overview pane, click **Widgets** and select a widget from the list:

- To add the pane into the upper left pane of the page, click the widget to be added.

- To add the pane to a specific pane on the page, drag 'n drop the widget into the desired pane.

Repeat this step to add additional widgets, up to a maximum of nine, to the overview page.

ℹ **NOTE:** You can use the links in the Filter By pane to filter the widget list. For example, to see only the widgets that pertain to agent status, click the **Agent Status** link. To redisplay all of the widgets available, click the **All Widgets** link at the top of the Widgets pane.

5   Once you have selected the widgets to be included, click the **Close** button (X) to collapse the widgets list pane and view the newly created overview page.

6   To rearrange the overview panes on the page, click in the heading of a pane and drag it to the new location on the page.

7   To change the content or format of an overview pane, click the edit button in the upper right corner of the pane.

Selecting this button displays parameters that can be used to customize the individual pane. Once you have selected your parameters, click **OK** to save your selection and close the parameter pane.

8   To remove a pane from the current view, click the X icon in the upper right corner of the pane.

9   Click the arrow icon and select **Shared Overviews** to return to the Shared Overviews Administration page. The newly created overview is now listed.

To email a link to a shared overview:

1   Once a shared overview has been created, use the **Email** toolbar button to share the overview with others.

- From the Shared Overviews Administration page, select the overview to be shared and click **Email**.

- From the individual overview page (in edit mode), click **Email**.

A new email is created which contains a direct link to the shared overview's web page.

2   Enter the recipient's email address and edit the Subject line if desired.

3   Click **Send**.

4   When the recipient receives notification, they simply click the link in the email and enter their user credentials on the logon page to view the shared overview.

> **i** | **NOTE:** The local computer must have an email client installed to use the Email toolbar button. In cases where an email client is not installed, select the overview to be shared, double-click or click **View**, copy the URL from the new tab that opens, and share it with the necessary users.

To view a shared overview as a Change Auditor Administrator or Operator:

1   From the Shared Overviews Administration page, select the shared overview to be viewed.

2   Double-click or click **View**.

A new tabbed page appears allowing you to view the contents of the selected overview.

> **i** | **NOTE:** This is a read-only page and cannot be edited. Use the **Edit** tool bar button back on the Shared Overviews Administration page to edit the overview page.

3   Click the close button on this page's tab to close the page.

To view a shared overview as a member of the ChangeAuditor Web Shared Overview Users group:

> **i** | **NOTE:** Users who are members of only the ChangeAuditor Web Shared Overview Users group only have permissions to view the read-only shared overview pages. If they attempt to access the main Change Auditor Web Client URL, an error is presented saying "You're not authorized to view this page." This is expected behavior. A Change Auditor adminitrator will need to share the URL of the specific shared overviews with these users.

1   Open the URL provided by your Change Auditor Administrator in a browser.

2   Provide your Windows credentials.

3   View the shared overview.

To edit a shared overview:

1   From the Shared Overviews Administration page, select the shared overview to be edited.

2   Click **Edit**.

An edit page appears allowing you to modify the selected overview.

- Use the **Widgets** button to add or remove queries from the overview page.

- Optionally, use the **Rename** button to rename the shared overview. On the Rename dialog, enter the new name and click **OK** to save your selection and close the dialog.

3   Click the arrow icon and select **Shared Overviews** to save your changes and return to the Shared Overviews Administration page.

To copy a shared overview:

1   From the Shared Overviews Administration page, select the shared overview to be copied.

2   Click **Copy**.

3   On the Copy dialog, enter a name for the shared overview. Click **Save**.

4   To edit the copy, back on the Shared Overviews Administration page, select it and click **Edit**.

5   On the edit page, use the **Widgets** and **Rename** tool bar buttons to modify the selected overview page.

6   Click the arrow icon button and select **Shared Overviews** to save your changes and return to the Shared Overviews Administration page.

To delete a shared overview:

1 From the Shared Overviews Administration page, select one or more overview pages.

2 Click **Delete**.

3 Click **Yes** on the confirmation dialog.

   The Shared Overviews Administration page is updated, removing the deleted shared overviews from the list.

Searches Page

- Introduction
- Run searches
- Create custom searches
- Search Properties tabs

Introduction

The Searches page is similar to the Searches page in the Change Auditor Windows client, displaying all of your search definitions, both private and shared. It also displays the search criteria used in each search definition. Click the **Searches** link in the expanded left pane to display this page. The Searches page consists of the following panes:

Folders

The left pane displays a hierarchical view of the folders used to manage your search definitions.

This view initially displays the following folders:

- Quick Search: Select to define a query that is to be run but not saved. Unlike other custom queries, the search criteria is not saved unless you click **Save As** on one of the Search Properties tabs.
- Private: Contains personal custom queries that only you can see.
- Shared: Contains the predefined search definitions and can also be used to store public custom queries that all users can see.

Searches

The right pane displays a list of the search definitions contained in the folder selected in the Folders pane. The following information is displayed for each search definition:

Table 8. Searches list: Field descriptions

Field	Description
Type	Indicates whether the search is private or shared and whether alerting and/or reporting has been enabled: Private Search, Shared Search, Private Alert, Shared Alert or Report.
Alert	Indicates whether an alert has been enabled.
Report	Indicates whether reporting has been enabled.
Name	Displays the name assigned to the search definition.
Alert To	Displays the recipients specified to receive an alert email notification (SMTP) or the shared folder if that option is selected.
Alert Cc	Displays the 'carbon copy' recipients specified to receive an alert email notification.
Alert Bcc	Displays the 'blind carbon copy' recipients specified to receive an alert email notification.
Report To	Displays the recipients specified to receive a report as defined on the Report tab.

Table 8. Searches list: Field descriptions

Field	Description
Report Cc	Displays the 'carbon copy' recipients specified to receive a report email.
Report Bcc	Displays the 'blind carbon copy' recipients specified to receive a report email.

Search Properties tabs

The tabs located across the bottom of the screen define the criteria or properties which make up the selected search. See Search Properties tabs for a description of these tabs and more information on how to create a custom query.

Run searches

To run a search:

1   In the Folders pane, click the expand properties button (right) arrow to the left of a folder to expand the folder and display a hierarchy of folders.

2   Select a folder to display the list of search definitions stored in the selected folder (for example, **Shared | Built-In | All Events**).

When a folder is selected in the Folders pane, the right pane is populated with a list of the search definitions that are stored in the selected folder.

3   Select a search definition in the Searches list to populate the Search Properties tabs at the bottom of the page. Click on a tab to view or edit the search criteria defined.

4   Use one of the following methods to run a search:

  ▪   Double-click the search definition

  ▪   Right-click the search definition and select **Run**

  ▪   Select the search definition and click the **Run** tool bar button at the top of the Searches page or from one of the Search Properties tabs

5   A new Search Results page is added which contains the events that met the search criteria defined in the selected search definition.

Create custom searches

You can create custom search definitions to audit the configuration changes that need to be tracked in your environment. You will use the Search Properties tabs, located across the bottom of the Searches page, to define new custom searches or edit existing search definitions.

ℹ | **NOTE:** The following procedure provides the general steps involved in creating a custom search using the web client. Refer to Search Properties tabs for more information on specifying search criteria on the individual tabs.

To create a new search:

1   Open the Searches page.

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

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

3   Click **New Search** at the top of the Searches page to activate the Search Properties tabs.

4   On the Search Properties tabs, enter the search criteria to be used. The following table provides a brief description of the tabs available and how to define criteria on each of these tabs.

ℹ **NOTE:** When you specify criteria on more than one Search Properties tab (e.g. Who, What and Where tabs), Change Auditor first evaluates each individual tab's criteria and then chains the individual tab's criteria together using the 'AND' operator, returning only those events that meet all of the search properties specified on the different tabs.

Table 9. Search Properties tabs

Tab	Description	How to add criteria
Info	Name your search	1 Enter name of search 2 Optionally enter description 3 Optionally select **Show as Widget** check box
Who	Search for events generated by a specific user, computer or group. By default, Change Auditor searches for events generated by all users, computers and groups.	1 Click **Add** to display Add Users, Computers, or Groups dialog. 2 On **Select User** tab, use Browse or Search page to locate and select the user, computer or group 3 Click **Add** to add criteria to selection list 4 Click **OK** to save selection and close dialog **NOTE:** Use the **Add Wildcard** tab to specify a wildcard expression to search for users or groups. **NOTE:** Use the **Add With Events** tab to select a user, computer or group that already has an event associated with it in the database.

Table 9. Search Properties tabs

Tab	Description	How to add criteria
What	Search for events based on subsystem, event class, object class, severity or result. By default, all entities are included in a new search definition.	1 Expand **Add** and select an option from the drop-down menu 2 On the Add tab, specify or select the 'what' criteria (depending on dialog): ▪ **Event Class** - Add Facilities or Event Classes dialog ▪ **Object Class** - Add Object Classes dialog ▪ **Severity** - Add Severities dialog ▪ **Result** - Add Results dialog ▪ **Active Directory** - Add Active Directory Container dialog ▪ **Azure Active Directory** - Add Azure Active Directory dialog. ▪ **AD Query** - Add Active Directory Container dialog ▪ **ADAM (AD LDS)** - Add ADAM (AD LDS) Container dialog ▪ **Exchange** - Add Exchange Container dialog ▪ **Office 365 Exchange Online** - Office 365 Exchange Online dialog ▪ **File System** - Add File System Path dialog ▪ **Group Policy** - Add Group Policy Container dialog ▪ **Local Account** - Add Local Account dialog ▪ **Logon Activity** - Add Logons dialog ▪ **Registry** - Add Registry Key dialog ▪ **Service** - Add Service dialog ▪ **SharePoint** - Add SharePoint Path dialog ▪ **SQL** - Add SQL Instance dialog ▪ **SQL Data Level** - Add SQL Data Level object ▪ **VMware** - VMware dialog 3 Click **Add** to add criteria to selection list 4 Click **OK** to save selection and close dialog **NOTE:** Use the **Add With Events** tab (instead of the **Add** tab) on these dialogs to select from a list of objects that already have an event associated with it in the database.

Table 9. Search Properties tabs

Tab	Description	How to add criteria
Where	Search for events captured by a specific agent or within a specific domain or site. By default, all agents will be included in a new search.	1 Click **Add** to display the Add Agents, Domains, Sites dialog 2 On the **Select Object** tab, use the Browse or Search page to locate and select an agent, domain or site 3 Click **Add** to add criteria to selection list 4 Click **OK** to save selection and close dialog **NOTE:** Use the **Add Agents** tab to select an agent from a list. **NOTE:** Use the **Add Wildcard** tab to specify a wildcard expression to search for domains, sites or agents. **NOTE:** Use the **Add With Events** tab to select agents, domains or sites that already have an event associated with it in the database.
When	Search for events that occurred during a specific date/time range. By default, new searches will include the events captured this week.	1 In Date Interval pane, select the date interval to be used and use controls to specify date interval 2 Optionally use the Time Interval controls to specify a start and end time
Origin	Search for events originating from a specific workstation or server. By default, Change Auditor searches for all events regardless of where they originated.	1 Click **Add** to display the Add Origin dialog. 2 On the **Add Wilcard** tab, enter a wildcard expression to search for a workstation or server. 3 Click **Add** to add criteria to selection list 4 Click **OK** to save selection and close dialog **NOTE:** Use the **Add With Events** tab to select an originating workstation/server that already has an event associated with it in the database.

5 If you want to be notified when an event is captured as a result of this custom search, open the Alert tab to enable and define how and where to dispatch alerts. See Alert tab for more information.

6 If you want to send reports for this query, open the Report tab to enable reporting and define the report recipients. See Report tab for more information.

7 Once you have defined the search criteria to be used, you can save and/or run the search query, using one of the following tool bar buttons at the top of most Search Properties tabs:

▪ **Save**: Saves the search definition without running it.

▪ **Save As**: Allows you to save the search definition to a different location within the folder hierarchy or using a different name.

▪ **Run**: Saves and runs the search. A new Search Results page will be added to the web client populated with the events that met the search criteria defined.

Search Properties tabs

Use the Search Properties tabs to view or define search criteria. The following sections provide a description of the fields/controls on each tab:

- **Info tab**: Allows you to enter a name and description for the search.
- **Who Tab**: Allows you to search for events generated by a specific user, computer or group.
- **What tab**: Allows you to search for events based on subsystem, event class, object class, severity or result.
- **Where tab**: Allows you to search for events captured by a specific agent, domain or site.
- **When tab**: Allows you to search for events that occurred within a specific date/time range.
- **Origin tab**: Allows you to search for events that originated from a specific workstation or server.
- **Alert tab**: Allows you to enable alerts for this query and define how and where to dispatch alerts.
- **Report tab**: Allows you to enable reporting for this query and define the report recipients.
- **Layout tab** - Allows you to define the data (columns) to be retrieved from the database and the sort order for displaying the retrieved data.

In addition, the following tabs can be displayed by selecting the appropriate check box on the Searches tab of the Client Settings dialog:

- **SQL tab** - Displays the SQL script used to create the selected search definition.
- **XML tab** - Displays the XML representation of the search criteria.

i | **NOTE:** To hide the Search Properties tabs, click the down arrow on the divider bar between the Searches List and Search Properties tabs. To show these tabs again, click the up arrow on the divider bar at the bottom of the screen.

Info tab

Use the Info tab to view or enter the name and description of a search definition. In addition, you can specify to add this search definition as a widget on the Overview page (Custom Views mode) or a Shared Overview.

Search Name

Displays the name of the selected search.

When creating a new search, place your cursor in this text box and enter a descriptive name for the search.

Search Description

Displays the description of the selected search.

To add a description to a new search, place your cursor in this text box and enter a brief description for the search.

Show as Widget

Select this check box to add this query as a widget on the widgets list on the Overview (Custom Views mode) and Shared Overviews pages.

Search Limit

This check box is checked by default and indicates the maximum number of records to be retrieved and displayed by the client. By default, the maximum of 50,000 records will be returned from the database during a single request. Use the arrow controls to change the search limit for the selected search.

NOTE: Clearing this check box removes the search limitation returning the events generated over for the last year, which may increase both client memory and wait time if expected search results are over 100,000. Therefore, it is highly recommended that you leave this check box checked and use the defined search limit.

Who Tab

Use the Who tab to view or define the users, computers and/or groups to be included in (or excluded from) the search definition. When multiple 'who' criteria is specified on this tab, Change Auditor uses the 'OR' operator to evaluate events, returning events for activity performed by any of the users, computers or groups listed.

NOTE: You can add a Group to a search to find all events made by the members of that group. Change Auditor must expand and store the membership of the group before all expected events are returned when the search is executed. When the search is saved, Change Auditor will expand the Group if it has not already been expanded. This may take several minutes, depending on your environment. Refer to the Coordinator Configuration page for the options available regarding group expansion.

NOTE: Activity performed by any accounts specified in an Excluded Accounts template will not be captured for the agents to which this template is assigned. Thus, Change Auditor will not return any events for these excluded accounts even if you specify them in the 'who' search criteria. Refer to Excluded Accounts auditing for more information on excluding accounts.

The Who tab contains the following information/controls:

Runtime Prompt

Select this check box to prompt for the 'who' criteria when this search is executed. That is, when you select **Run**, the Add Users, Computers, or Groups dialog is displayed allowing you to locate and select the users, computers, or groups to search.

NOTE: When this check box is checked, the **Add** tool bar button will be deactivated.

NOTE: You can not enable alerting for search definitions that use the **Runtime Prompt** option.

Include Event Source Initiator

If you are running Active Roles Server or GPOADmin and want to include events generated by Active Roles or GPOADmin in the search, select this check box. Selecting this check box instructs Change Auditor to retrieve all events made by the specified user account, including those initiated by Active Roles and GPOADmin.

NOTE: An additional column (Initiator UserName) is added to the Search Results grid to display the user account that initiated the change using Active Roles or GPOADmin.

For more information, see the Active Roles Server Integration and GPOADmin Integration appendices in the Change Auditor Installation Guide.

Exclude the Following Selection(s)

Select this check box to specify the users, computers or groups to be excluded from the search. That is, Change Auditor is to search on all users, groups and computers except those listed.

Who list

By default, all users, computers and groups will be included in a new search definition and therefore this list will be empty.

Once criteria is selected, the Who list box will contain the individual users, computers and/or groups to be included in the search (or excluded from the search if the **Exclude the Following Selection(s)** option is checked).

Add Users, Computers, or Groups dialog

Clicking **Add** on the Who tab displays the Add Users, Computers, or Groups dialog allowing you to select the user, computer or group to be included in a custom search. Use the tabbed pages on this dialog as described below.

Table 10. Add Users, Computers, or Groups dialog

Tabs	How to add criteria
Select User	*To search for events generated by a specific directory object:* 1 Use the Browse or Search page to search your environment to locate and select the user, computer or group to be included. 2 Click **Add** to add criteria to the selection list 3 Repeat to include each additional directory object 4 Click OK to save your selections and close the dialog.
Add Wildcard	*To use a wildcard expression to specify a user or group:* 1 Select the comparison operator to be used: **Like** or **Not Like** 2 In the text box, enter the pattern (character string and * wildcard character) to be used to search for a match. Use the * wildcard character to match any string of zero or more characters. For example, **LIKE *admin*** will find all users with the character string 'admin' anywhere in the name. 3 By default, the wildcard expression will be used to search for a user. To search for a group, select the **Group** option. 8 Click **Add** to add criteria to the selection list. 4 Click **OK** to save your selections and close the dialog
Add With Events	*To search for events generated by a directory object that already has an event in the database:* 1 Select one or more directory objects from the list. 2 Click **Add** button to add criteria to the selection list. 3 Click **OK** to save your selections and close the dialog.

What tab

Use the What tab to define 'what' entities are to be included (or excluded) in the search. More specifically, using this tab you can create a search for events based on:

- Event Class
- Object Class
- Severity
- Result
- Subsystem (such as Active Directory, Exchange, Group Policy, and SQL)

When criteria is specified on the What tab, Change Auditor will retrieve only those events that match the criteria listed on the What tab. When multiple 'what' criteria is specified on this tab, Change Auditor uses the 'AND' operator to evaluate an event and returns only those events that meet all the specified criteria. However, when multiple subsystems (for example, Active Directory, ADAM and Exchange) are specified, Change Auditor uses the 'OR' operator to evaluate these entities, returning events that meet any of the specified subsystem criteria. This also applies when multiple event classes are specified. That is, when multiple event classes are specified, Change Auditor uses the 'OR' operator and returns any of the specified events.

By default, all events will be included in a new search definition and therefore the list box on the What tab will be empty. Once criteria is added, the list box contains an expandable view displaying the criteria defined for the search definition.

> **i** | **NOTE:** Click the expansion box to the left of the What field to expand this view and display additional details, which are dependent on the type of entity.

Add dialogs

To add an entity to the What list, expand the **Add** command and select the appropriate option. On the dialog that appears, specify the 'what' criteria for your search. The following table provides a list of the **Add** command options available with a brief description, the dialog that is displayed and the criteria that can be specified on each of these dialogs.

> **i** | **NOTE:** The different Change Auditor auditing modules must be licensed in order to capture and retrieve their associated events. See the **License Required** column in the table below to see the Change Auditor license required.

Table 11. What tab: Add command options/dialogs

Add command option	License required	Description, dialog and criteria

Event Class	Any	Select to search for events based on the event class or facility to which they belong.
		Add Facilities or Event Classes dialog:
		1 Select an event class from the list.
		2 Click **Add** and select one of the following options:
		   ▪ Add This Event
		   ▪ Add All Events in Facility
		3 If 'Add Restrictions' appears in the Restriction cell, optionally, click in the cell to add restrictions pertaining to that event class.
		4 Click **OK** to save selection and close dialog.
		NOTE: Use **Add With Events** to limit the list to events that already have an event in the database.

Object Class	Change Auditor for Active Directory	Select to search for changes to specific object classes (classSchema objects). **Add Object Classes dialog**: 1 Select an object class from the list. 2 Click **Add**. 3 Click **OK** to save selection and close dialog. **NOTE:** Use **Add With Events** to limit the list to object classes that already have an event in the database.
Severity	Any	Select to search for events based on the severity assigned. **Add Severities dialog**: 1 Select a severity from the list. 2 Click **Add**. 3 Click **OK** to save selection and close dialog. **NOTE:** Use **Add With Events** to limit the list to severities that already have an event associated with it in the database.

Table 11. What tab: Add command options/dialogs

Add command option	License required	Description, dialog and criteria
Result	Any	Select to search for events based on the results of the operation mentioned in the event. **Add Results dialog**: 1 Select a result from the list. 2 Click **Add**. 3 Click **OK** to save selection and close dialog. **NOTE:** Use **Add With Events** to select from a list of results that already have an event associated with it in the database.

Active Directory	Change Auditor for Active Directory	Select to search for changes to objects in selected Active Directory containers.
		
		Add Active Directory Container dialog:
		1 Use the Browse or Search page to locate and select an Active Directory container.
		
		    You can also select **Import Objects** to import a .csv file of a list of directory objects. Using this list, you can search for an exact object name or use a wildcard.
		
		    The first row of the .csv file must be column names and the first column must be NAME.
		2 Click **Add** to add to selection list.
		3 Click in **Scope** cell to change the scope of the search.
		4 Click in **Actions** cell to change setting. **All Actions** is selected by default, meaning all activity associated with the object will generate an event.
		
		    To select individual actions, you must first clear the **All Actions** check box.
		5 Click in **Transports** cell to change setting. **All Transports** is selected by default, meaning all AD query operations regardless of the transport protocol used will be included in the search.
		
		    To select individual transports, you must first clear the **All Transports** check box.
		6 Click **OK** to save selections and close dialog.
		
		NOTE: Use **Add Wildcard** to specify a wildcard expression to search for Active Directory objects.
		
		NOTE: Use **Add With Events** to select from a list of Active Directory containers that already have an event associated with it in the database.
		
		NOTE: Use **Add Enterprise** to add the enterprise to the selection list. When this option is selected, all other containers in the selection list are ignored (appear in red). Also, the scope setting cannot be changed.

Table 11. What tab: Add command options/dialogs

Add command option	License required	Description, dialog and criteria
AD Query	Change Auditor for Active Directory Queries ChangeAuditor for LDAP (v 5.x)	Select to search for a specific Active Directory query that was performed against a specified Active Directory object. **Add Active Directory Container dialog**: 1 Use the Browse or Search page to locate and select an Active Directory container. 2 Click **Add** to add to selection list. 3 Click in **Scope** cell to change the scope of the search. 4 Click in **Filter** cell to search for an LDAP filter string used in an Active Directory query. 5 Click in **Attributes** cell to search for attributes that are being queried. 6 Click in **Results** cell to search for queries that return a specific number of results. 7 Click in **Elapsed** cell to search for queries that take a specific amount of time to complete. 8 Click in **Transports** cell to change setting. **All Transports** is selected by default, meaning all Active Directory queries regardless of the transport protocol used will be included in the search. To select individual transports, you must first clear the **All Transports** check box. 9 Click **OK** to save selections and close dialog. **NOTE:** Use **Add With Events** to select from a list of objects that already have an event in the database. **NOTE:** Use **Add Enterprise** to search the entire enterprise. When this option is selected, all other objects in the selection list are ignored (appear in red). Also, the scope, filter, attributes, results and elapsed settings cannot be changed.

Table 11. What tab: Add command options/dialogs

Add command option	License required	Description, dialog and criteria
ADAM (AD LDS)	Change Auditor for Active Directory	Select to search for changes to objects in selected ADAM (AD LDS) containers. **Add ADAM (AD LDS) Container dialog**: 1 Select **CHOOSE COMPUTER** link. 2 On the Select the agent that hosts the ADAM/AD LDS Instance dialog, use the Browse or Search page to locate and select the ADAM instance. 3 Click **OK** to browse the selected instance. If prompted, enter the credentials to be used to access the selected ADAM (AD LDS) instance. 4 Select an object from the list. 5 Click **Add** to add to selection list. 6 Click in **Scope** cell to change the scope of the search. 7 Click in **Actions** cell to change setting. **All Actions** is selected by default, meaning that all activity associated with the object will generate an event. To select individual actions, you must first clear the **All Actions** check box. 8 Click in **Transports** cell to change setting. **All Transports** is selected by default, meaning that all AD query operations regardless of the transport protocol used will be included in the search. To select individual transports, you must first clear the **All Transports** check box. 9 Click **OK** to save selection and close dialog. **NOTE:** Use **Add With Events** to select from a list of ADAM (AD LDS) containers that already have an event associated with it in the database. **NOTE:** Use **Add Enterprise** to search the entire enterprise. When this option is selected, all other containers in the selection list are ignored (appear in red). Also, the scope setting cannot be changed.

Table 11. What tab: Add command options/dialogs

Add command option	License required	Description, dialog and criteria
Azure Active Directory **NOTE:** When Azure Active Directory events include multiple targets, Change Auditor identifies these as Target (primary target) and Subject (secondary target).	Change Auditor for Active Directory	Select to search for changes in Azure Active Directory. **Add Azure Active Directory dialog**: 1 Select the Category filter to specify the event category to include in the search. Select a comparison operator (**Like** or **Not like**) and enter a category name. For example, for activities related to self-service password resets, choose the "Self-service Password Management" category. 2 Select the Activity Type filter to specify the activity to include in the search. Select a comparison operator (**Like** or **Not like**) and enter an activity type. For example, for user related activities, select "User" as the activity type. 3 Select the Activity Name filter to specify the activity to include in the search. (For sign-in risk events, this shows the detected activity that occurred on the risk event.) Select a comparison operator (**Like** or **Not like**) and enter an activity name (character string and the * wildcard character). For example: Like *delete* searches for events where Activity contains 'delete'. For a list of all available activities, see the Microsoft article "Audit activity reports in the Azure Active Directory portal". 4 Select the Activity Details filter to include activity details in the search. (For sign-in risk events use the status of the risk event, such as Resolved). Select a comparison operator (**Like** or **Not like**) and enter a full or partial string (character string and the * wildcard character). For example, the 'Self-serve password reset flow activity progress' activity provides several different details including: User started the mobile SMS verification option, User started the e-mail verification option, or User successfully reset password. Leave this filter blank to return events for all activities or narrow the search based on the activity details.

Table 11. What tab: Add command options/dialogs

Add command option	License required	Description, dialog and criteria
		5 Select the Target filter to specify the target (primary and secondary targets) to include in the search. (For sign-in risk events, the field searches for the risk event type such as Sign-in from anonymous IP address). Select a comparison operator (**Like** or **Not like**) and enter a full or partial name (character string and the * wildcard character). The Target filter searches across the following properties: Object Name (Cloud Target Name), Target Display Name, On-Premises Target, Subject Name, Subject Display Name, and On-Premises Subject.
		6 Select the Activity Origin filter to specify the activity origin to include in the search. You can choose between Cloud (event activity was performed directly in the cloud) or AD (event activity was originally performed on-premises and was synchronized to the cloud).
		7 Select the Sync Type filter to specify the target (primary and secondary targets) synchronization type to include in the search. You can choose between In Cloud (target object exists only in the cloud) and Synced from AD (target object was synchronized from Active Directory)
		8 Click **Add** to add the expression to the selection list.
		9 Repeat this process to add any additional expressions to the search query.
		NOTE: Use **Add Wildcard** to specify a wildcard expression to search for Azure Active Directory changes.
		NOTE: Use **Add With Events** to select from a list of Azure Active Directory changes that already have an event associated with it in the database.
		NOTE: Use **Add all events** to add all Azure Active Directory events.
		NOTE: When multiple entries are added to the selection list, Change Auditor uses the 'OR' operator to evaluate events, returning events that meet any of the entries listed.

Table 11. What tab: Add command options/dialogs

Add command option	License required	Description, dialog and criteria
Exchange	Change Auditor for Exchange	Select to search for changes to objects in selected Exchange containers.

Add Exchange Container dialog:

1 Use the Browse or Search page to locate and select an Exchange container.

You can also select **Import Objects** to import a .csv file of a list of directory objects. Using this list, you can search for an exact object name or use a wildcard.

The first row of the .csv file must be column names and the first column must be NAME.

2 Click **Add** to add to selection list.

3 Click in **Scope** cell to change the scope of the search.

4 Click in **Actions** cell to change setting. **All Actions** is selected by default, meaning all activities associated with the object will generate an event.

To select individual actions, you must first clear the **All Actions** check box.

5 Click in **Transports** cell to change setting. **All Transports** is selected by default, meaning that all AD query operations regardless of the transport protocol used will be included in the search.

To select individual transports, you must first clear the **All Transports** check box.

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

NOTE: Use **Add Wildcard** to specify a wildcard expression to search for Exchange containers.

NOTE: Use **Add With Events** to select from a list of Exchange containers that already have an event associated with it in the database.

NOTE: Use **Add Enterprise** to search the entire enterprise. When this option is selected, all other containers in the selection list are ignored (appear in red). Also, the scope setting cannot be changed.

Table 11. What tab: Add command options/dialogs

Add command option	License required	Description, dialog and criteria
Office 365 Exchange Online **NOTE:** Use **Add With Events** to select from a list of Exchange Online mailboxes that already have an event associated with them in the database. **NOTE:** Expand **Add All** and select one of the following to search for 'all' Office 365 Exchange Online events: **All Office 365 Exchange Online Events**, **All Office 365 Exchange Online Mailbox Events**, or **All Office 365 Exchange Online Administration Events**. When one of these options is selected, all other entries in the selection list are ignored (appear in red).	Change Auditor for Exchange	Select to search for changes to a specific Exchange Online mailbox. **Office 365 Exchange Online dialog:** 1 Select whether you are adding a Mailbox or Cmdlet event. 2 If **Mailbox Event** is selected: To search for changes to a specific mailbox or a specific folder in all monitored mailboxes: ▪ Select **Mailbox Name** and/or **Folder Name**, select the comparison operator to be used: **Contains** or **Does not contain**. Enter the name (or partial name) of a mailbox/folder to be used to search for a match. (Case sensitivity is based on your SQL setting). Click **Add** to add criteria to selection list. If both the **Mailbox Name** and **Folder Name** are specified, both expressions must be met. To search for changes by specific on-premises users: ▪ Select **On-Premises User Name**, select the comparison operator to be used: **Like** or **Not like** and enter the name (or partial name) to be used to search for a match. (Case sensitivity is based on your SQL setting.) Click **Add** to add the criteria to the selection list. To search for changes for specific targets (either based on the SAM account and domain name of the on-premises mailbox account that corresponds to the cloud-based mailbox account or based on the mailbox account display name): ▪ Select **On-Premises Target Name or Target Display Name,** select the comparison operator to be used: **Like** or **Not like** and enter the name (or partial name) to be used to search for a match. Case sensitivity is based on your SQL setting. Click **Add** to add the expression to the selection list. To search for changes in mailbox accounts based on how they are synchronized: ▪ Select **Target Sync Type,** select **In cloud** to include mailbox accounts created in the cloud or **Synced from AD** to include mailbox accounts that have been synchronized from your on-premises Active Directory directories. Click **Add** to add the expression to the selection list. **NOTE:** When multiple entries are added to the selection list, Change Auditor uses the 'OR' operator to evaluate events, returning events that meet any of the entries listed.

Table 11. What tab: Add command options/dialogs

Add command option	License required	Description, dialog and criteria
		If **Administration Cmdlet Event** is selected:
		• Select **Cmdlet** and/or **Cmdlet Object** check box.
		• Select the comparison operator to be used: Contains or Does not contain.
		For Cmdlet, enter the 'command' to be used to search for a match. For Cmdlet Object, enter the name (or partial name) of a mailbox to be used to search for a match. Case sensitivity is based on your SQL setting.
		• Click **Add** to add criteria to selection list.
		If both the Cmdlet and Cmdlet Object are specified, both expressions must be met.
		• Click **OK** to save the selection and close the dialog.
File System	One of the following:	Select to search for specific file system events.
	Change Auditor for Windows File Systems	**Add File System Path dialog**:
		1 Enter a file or folder path.
	Change Auditor for NetApp	2 Click **Add** to add to selection list.
		3 Click in **Scope** cell to change the scope of the search.
	Change Auditor for EMC	4 Click in **Actions** cell to change setting. **All Actions** is selected by default, meaning that all activity associated with the file system will be included in the search.
		To select individual actions, you must first clear the **All Actions** check box.
		5 Click in **Types** cell to change setting. **All Types** is selected by default, meaning all file system path types will be searched.
		6 Click **OK** to save selections and close dialog.
		NOTE: Use **Add With Events** to select from a list of file system paths that already have an event associated with it in the database.
		NOTE: Use **Add All File System Paths** to search all file system paths. When this option is selected, all other file system paths in the selection list are ignored (appear in red). Also, the Scope and Types settings cannot be changed.

Table 11. What tab: Add command options/dialogs

Add command option	License required	Description, dialog and criteria
Group Policy	Change Auditor for Active Directory	Select to search for changes to objects in selected Group Policy containers. **Add Group Policy Container dialog**: 1 Use the Browse or Search page to locate and select a Group Policy container. You can also select **Import Objects** to import a .csv file of a list of directory objects. Using this list, you can search for an exact object name or use a wildcard. The first row of the .csv file must be column names and the first column must be NAME. 2 Click **Add**. 3 Click **OK** to save selections and close dialog. **NOTE:** Use **Add Wildcard** to specify a wildcard expression to search for Group Policy containers. **NOTE:** Use **Add With Events** to select from a list of Group Policy containers that already have an event associated with it in the database. **NOTE:** Use **Add All Group Policies** to search all group policies in the enterprise. When this option is selected, all other containers in the selection list are ignored (appear in red).
Local Account	Any	Select to search for changes to users or groups that reside in local SAM databases of a member server. **Add Local Account dialog**: 1 Select a user or group account from the list. 2 Click **Add**. 3 Click **OK** to save selections and close dialog. **NOTE:** Use **Add All Local Accounts** to search all local accounts in the enterprise. When this option is selected, all other accounts in the selection list are ignored (appear in red).
Logon Activity	Change Auditor for Logon Activity User for server agents Change Auditor for Logon Activity Workstation for workstation agents	Select to search for a specific type of logon event. **Add Logons dialog:** 1 Select a logon type from the list. 2 Click **Add**. 3 Click **OK** to save selections and close dialog. **NOTE:** Use **Add With Events** to select from a list of logon types that already have an event in the database.

Table 11. What tab: Add command options/dialogs

Add command option	License required	Description, dialog and criteria
Registry	Any	Select to search for changes to system registry keys that already have an event associated with it in the Change Auditor database. **Add Registry Key dialog**: 1 Select a registry path from the list. 2 Click **Add**. 3 Click in **Scope** cell to change the scope of the search. 4 Click in **Actions** cell to change setting. **All Actions** is selected by default, meaning all registry key actions will be included in the search. To select individual actions, you must first clear the **All Actions** check box. 5 Click **OK** to save selections and close dialog. **NOTE:** Use **Add All Registry Keys** to search all registry keys in the enterprise. When this option is selected, all other registry keys in the selection list are ignored (appear in red). In addition, the Scope cannot be changed.
Service	Any	Select to search for changes to services which already have an event associated with it in the Change Auditor database. **Add Service dialog**: 1 Select a service from the list. 2 Click **Add**. 3 Click **OK** to save selections and close dialog.
SharePoint	Change Auditor for SharePoint	Select to search for changes to specific SharePoint components. **Add SharePoint Path dialog**: 1 Select a path from the hierarchy displayed. 2 Click **Add**. 3 To specify a wildcard expression to search for events generated against specific SharePoint components: - Click the appropriate cell in the selection list (Farm Name, Web Name, List Name, Item Name, or Item URL). - Select the check box on the displayed dialog to enable the controls. - Select the comparison operator: **Like** or **Not Like**. - Enter the pattern (character string and * wildcard character) to be used to search for a match. You can also use **Add Wildcard** to specify wildcard expressions. 4 Click **OK** to save selections and close dialog. **NOTE:** When multiple wildcard expressions are specified, they are 'ANDed' together and all of the expressions must be met to be considered a match. **NOTE:** Use **Add With Events** to limit this list to SharePoint paths that already have an event associated with it in the database. **NOTE:** Use **Add All SharePoint Paths** to search all SharePoint paths in the enterprise. When this option is selected, all other paths in the selection list are ignored (appear in red).

Table 11. What tab: Add command options/dialogs

Add command option	License required	Description, dialog and criteria
SQL	Change Auditor for SQL Server	Select to search for changes to specific SQL instances. **Add SQL Instance dialog**: **NOTE:** At least one of the fields (Instance, Database or SQL Object) must be specified. 1 Instance: Enter the name of the SQL instance to be searched. If left blank, Change Auditor searches all SQL instances. 2 Database: Enter the name of the SQL database to be searched. If left blank, Change Auditor searches all audited SQL databases. 3 SQL Object: Enter a SQL Server object to be included in the search. If left blank, Change Auditor searches for all audited SQL Server objects. 4 Click **Add** to add criteria to selection list. 5 Click **OK** to save selections and close dialog. **NOTE:** Use **Add With Events** to select from a list of SQL instances that already have an event associated with it in the database. **NOTE:** Use **Add All SQL Instances** to search all SQL instances in the enterprise. When this option is selected, all other instances in the selection list are ignored (appear in red).
SQL Data Level	Change Auditor for SQL Server	On the Add SQL Data Level Object, select one of the following and enter the search term: • Application Name • Database Name • Table Name • Transaction ID 1 Once you have specified the search term, click **Add** to add it to the Selection list at the bottom of the dialog. 2 Click **OK** to save your selection and close the dialog.

Table 11. What tab: Add command options/dialogs

Add command option	License required	Description, dialog and criteria
VMware	Any	Select to search for changes to a specific VMware host or virtual machine. **VMware dialog:** 1 Select the **Host Name** and/or **VM Name** check box: 2 If the **Host Name** check box is selected: - Select the comparison operator: **Like** or **Not Like**. - Enter the full name of the VMware host (vCenter® Server or individual host computer) or a pattern (character string and * wildcard character). 3 If the **VM Name** check box is selected: - Select the comparison operator: **Like** or **Not Like**. - Enter the full name of the virtual machine or a pattern (character string and * wildcard character). If both the **Host Name** and **VM Name** are specified, both expressions must be met. 4 Click **Add** to add criteria to selection list. 5 Click **OK** to save selections and close dialog. **NOTE:** Use **Add With Events** to select from a list of items that already have an event in the database. **NOTE:** Use **Add All VMware Hosts** to add all hosts. When this option is selected, all other items in the selection list are ignored (appear in red).

Where tab

The Where tab allows you to specify which agents to include (or exclude) in the search definition. You can select individual agents, all agents in a specific domain, or a given site. When multiple 'where' criteria is added to this tab, Change Auditor uses the 'OR' operator to evaluate change events, returning events captured by any of the specified agents, domains, or sites.

The Where tab contains the following information and controls:

Runtime Prompt

Select this check box to prompt for the 'where' criteria when this search is executed. That is, when you select **Run**, the Select one or more Directory Objects dialog appears allowing you to locate and select the agents, domains, or sites to include in the search definition.

> **NOTE:** When this check box is checked, the **Add** tool bar button will be deactivated.

> **NOTE:** You can not enable alerting for search definitions that use the **Runtime Prompt** option.

Exclude the Following Selection(s)

Select this check box to specify the agents, domains or sites to be excluded from the search. That is, Change Auditor is to return events generated from all agents except those listed in the Where list.

Where list

By default, all agents will be included in a new search and therefore this list box will initially be empty.

Once criteria is selected, the Where list box will contain the agents, domains, and sites to be included in the search (or excluded from the search if the **Exclude the Following Selection(s)** option is checked).

Add Agents, Domains, Sites dialog

Clicking the Add tool bar button displays the Add Agents, Domains, Sites dialog allowing you to specify the agent, domain or site to include in a custom search. Use the tabbed pages on this dialog as described below.

Table 12. Add Agents, Domains, Sites dialog

Tab	How to add criteria
Select Object	***To search for events captured by a specific agent, domain or site:***
	1 Use the Browse or Search pages to locate the directory object in your environment.
	2 Click **Add** to add criteria to the selection list.
	3 Repeat to add additional agents, domains or sites.
	4 Click **OK** to save your selections and close the dialog.
Add Agent	***To search for events captured by a specific agent:***
	1 Select an agent from the displayed list.
	2 Click **Add** to add criteria to the selection list.
	3 Repeat to add additional agents.
	4 Click **OK** to save your selections and close the dialog.
Add Server Type	***To filter based on server type:***
	1 Select to include Domain Controllers, Member Servers, Workstation Servers, Exchange Servers as required.
	2 Click **Add** to add criteria to the selection list.
	3 Click **OK** to close the dialog and add the server type to the 'Where' list.
	When this search runs, Change Auditor searches for events generated on the specified domains, sites, or agents for the specified server type.
Add Wildcard	***To use a wildcard expression to specify an agent, domain or site:***
	1 Select the comparison operator to be used: **Like** or **Not Like**.
	2 In the expression field, enter the pattern (character string and * wildcard character) to be used to search for a match (NetBIOS name). Use the * wildcard character to match any string of zero or more characters. For example, **LIKE *local** will find all agents whose NetBIOS name ends in 'local'.
	3 By default, the wildcard expression will be used to search for an agent. To search for a domain or site, select the **Domain** or **Site** option.
	4 Click **Add** to add the expression to the selection list.
	5 Click **OK** to save your selection and close the dialog.
Add With Events	***To search for events captured by an agent, domain or site that already has an event in the database:***
	1 Select one or more directory objects from the list.
	2 Click **Add** to add criteria to the selection list.
	3 Click **OK** to save your selections and close the dialog.

When tab

Use the When tab to define a date and/or time range in order to limit your search to include only those events that occur during the selected ranges.

The When tab contains the following information/controls:

Runtime Prompt

> Select this check box to prompt for the date and/or time interval each time this search is run. That is, when you select **Run**, the When dialog appears allowing you to specify the date/time interval to use in your search.
>
> > **i** | **NOTE:** When this check box is checked, the **Date Interval/Time Interval** settings will be deactivated.
>
> > **i** | **NOTE:** You can not enable alerting for search definitions that use the **Runtime Prompt** option.

Date Interval

> By default, a new search is set to include the events captured this week (Sunday at midnight, local time, through the current date and time).
>
> To change this setting, select one of the date interval options:
>
> - **From/To**: Select this check box and specify the starting and ending date for your date range. Click the calendar icon to select a date from the calendar control.
> - **Last**: Select this check box and the appropriate relative date and value (number of minutes, hours, days, weeks, months, quarters or years).
> - **This**: Select this option and click the arrow control to select the appropriate time interval (Day, Week or Month).

Time Interval

> Select the **Time Interval** check box to specify a time range to further limit your search.
>
> - **From**: Enter the starting time for your time range or click the clock icon to select a time from the list. Only events that occurred at or after this time will be included in the search.
> - **To**: Enter the ending time for your time range or click the clock icon to select a time from the list. Only events that occurred before or at this time will be included in the search.

Origin tab

Use the Origin tab to search for events based on the NetBIOS name or IP address of the workstation or server from which the event originated. When multiple 'origin' criteria is specified on this tab, Change Auditor uses the 'OR' operator to evaluate events, returning events that originated from any of the specified workstations or servers.

The Origin tab contains the following information/controls:

Runtime Prompt

> Select this check box to prompt for the originating workstation or server when this search is executed. That is, when you select **Run**, the Add Origin dialog appears allowing you to enter the wildcard expression to locate a specific workstation or server.
>
> > **i** | **NOTE:** When this check box is checked, the **Add** tool bar button will be deactivated.
>
> > **i** | **NOTE:** You can not enable alerting for search definitions that use the **Runtime Prompt** option.

Exclude the Following Selection(s)

Select this check box to specify the workstations or servers to be excluded from the search. That is, Change Auditor is to return events originating from all workstations and servers except those listed in the Origin list.

Origin list

By default, all events regardless of where they originated will be included in a new search and therefore this list box will initially be empty.

Once criteria is selected, the Origin list box will contain the wildcard expression used to locate workstations or servers to be included in the search (or excluded from the search if the **Exclude the Following Selection(s)** option is checked).

Add Origin dialog

Clicking **Add** displays the Add Origin dialog allowing you to specify an originating workstation or server. Use the tabbed pages on this dialog as described below.

Table 13. Add Origin dialog

Tab	How to add criteria
Add Wildcard	*To search for events based on where they originated:*
	1 Select the comparison operator to be used: **Like** or **Not Like**.
	2 In the Expression field, enter the pattern (character string and * wildcard character) to be used to search for a match (NetBIOS name or IP Address). Use the * wildcard character to match any string of zero or more characters.
	3 Click **Add** to add criteria to the selection list.
	4 Click **OK** to save your selection and close the dialog.
Add With Events	*To search for events originating from a workstation or server that has an event in the database:*
	1 Select one or more workstations/servers from the list.
	2 Click **Add** to add criteria to the selection list.
	3 Click **OK** to save your selection and close the dialog.

Alert tab

Use the Alert tab to enable an alert for the selected search definition and define how and where to dispatch the alert, via SMTP (email), SNMP and/or WMI.

> **i** | **NOTE:** You can NOT enable alerting for search definitions that use the **Runtime Prompt** option for one or more search criteria.

The Alert tab contains the following information/controls:

Alert Enabled

Select this check box to enable an alert for the current search definition. Clear this check box to disable the alert for the current search definition.

> **i** | **NOTE:** This check box becomes available only after you have selected at least one transport method in the **Send Alert To** pane on this tab.

Send Alert To

Select all of the transport options that are to be applied to this search definition:

- **SNMP**: Select to dispatch alerts via SNMP traps.

- **WMI**: Select to dispatch alerts via WMI (Windows Management Instrumentation).
- **SMTP**: Select to display alerts via email.

History Search Limit

By default, up to 50,000 events can be included in the alert history. Use the arrow controls to increase or decrease this value to define the maximum number of events to be included in the alert history.

SMTP | Configure Email

For SMTP alerts, select this button to display the Alert Custom Email dialog to change the details about the alert email to be sent, including:

- Events Per Email: Specify the maximum number of events to be included in a single email (Default is 100 events)
- Time Zone: Specify the time zone to be used for the alert's date/time stamps (Default is time zone of server where IIS is installed)
- To: Specify the email address of any users who are to receive the alert email.
- Cc: Specify the email address of any users who are to receive a carbon copy of the alert email.
- Bcc: Specify the email address of any users who are to receive a blind carbon copy of the alert email.
- Reply To: Enter the address where replies to alert emails are to be sent. By default, this setting used the value specified on the SMTP Configuration pane of the Coordinator Configuration page.
- Alert Subject: Specify the subject line text. By default, this setting uses the value specified on the SMTP Configuration pane of the Coordinator Configuration page.
- Send Plain Text Email | Send HTML Email: Specify the email format. By default, this setting uses the value specified on the SMTP Configuration pane of the Coordinator Configuration page.
- Add Who: Select this option to send an alert to the user who initiated the change that triggered the alert. Specify if this user is to be added to the To, Cc or Bcc address field.
- Add Owner(s): Select this option to send an alert to the Exchange Mailbox owner whose mailbox was accessed by another user and their action triggered an alert. Specify if this user is to be added to the To, Cc or Bcc address field.

  i | **NOTE:** This feature only applies to Exchange Mailbox Monitoring events, which are available in Change Auditor for Exchange.

- Add Managed By: For events associated with groups that are being manged by another account, select this option to send an alert to the managing user's email. Specify if this user is to be added to the To, Cc or Bcc address field.

SMTP | Configure Email | Configure Body

From the Alert Custom Email dialog, select **Configure Body** to display the Alert Body Configuration dialog where, after clearing the **Use Global Main Body** check box on th Main Body tab or the **Use the Global Event Details** check box on the Event Details tab, you can define the content of the main body and/or the event details to be included in your alert emails.

Smart Alert When

Select this check box to specify under what conditions an alert is to be sent. Use the controls below this check box to specify the number of events that must occur within a specified time interval (minutes, hours or days) before generating/dispatching the alert.

i | **NOTE:** This feature is available for SNMP and SMTP alerts only.

On a Single Object

Select this check box to specify that the event must occur for the same object the specified number of times before the alert will be triggered. When this check box is cleared (default), the event can occur on any object the specified number of times to trigger the alert.

Report tab

The Report tab allows you to enable reporting and define when and where to send the email report.

In addition to the standard tool bar buttons, the following buttons appear on the Report tab:

Preview Report

Click **Preview Report** to display a rendering of the events returned as a result of the selected search.

Design Report

Click **Design Report** to launch the Report Designer which allows you to create a custom report layout for the selected search.

> **i** | **NOTE:** Once the report designer is launched, the **Layout** and **Columns** settings on the Report tab for the selected search are disabled. To re-enable these settings, click the **Reset** button on the Report tab.

The Report tab consists of a Schedule tab and a Configuration tab which contain the following information/controls:

Report Enabled

Select this check box to enable reporting for the current search definition.

> **i** | **NOTE:** This option becomes available only after a valid email address is entered in the **To** field in the Report Configuration section of this tab.

Reset

Click **Reset** to reset the settings back to the factory defaults.

Last Run

This read-only field specifies the last time (date and time) the report ran.

Next Run

This read-only field specifies the next time (date and time) when the report is scheduled to run.

Schedule tab

The Schedule tab is used for setting the date and time a report is to be run.

Report

Specifies if the report is to be generated/sent on a weekly (default) or monthly schedule.

Every

When a **Weekly** report is selected, specifies the weekly schedule to be used to generate the report. For example, 1 for every week (default), 2 for every other week, 3 for every third week, and 4 for every fourth week.

When a **Monthly** report is selected, specifies the monthly schedule to be used to generate the report. For example, 1 for every month, 2 for every other month, and 3 for every three months.

On Days

When a **Weekly** report is selected, defines the days of the week when the report is to be generated. The default is Monday through Friday.

On Day of Month

When a **Monthly** report is selected, specifies on which day of month the report is to be generated:

- First (default)
- Last
- Day #

Run Time

Specifies the time at which the report is to be generated. By default, the report will be generated at 12:00 AM. Click the clock icon to the left of this field to select a time from a list.

Configuration tab

The Configuration tab is used for specifying the report's settings and the recipients.

Layout

Specifies what report template is to be used for the report's headers and footers. The **Default** report template has been defined for you. To define additional report templates, use the Report Layouts page on the Administration Tasks page.

i | **NOTE:** This setting is disabled if you click the **Design Report** tool bar button to define a custom report layout for the selected search.

Attach

The report is sent as an email attachment. Select the appropriate **Attach** option to define the format to be used for the report:

- PDF (default)
- HTML
- Word
- Text
- Excel
- CSV

Columns

Defines how the report content is to fill the page:

- Fit to Page (default)
- Fixed Width *nn.nn* inches/column

i | **NOTE:** These settings are disabled if you click the **Design Report** tool bar button to define a custom report layout for the selected search.

Time Zone

Specifies the time zone to be used for the report's time stamp in the report email. By default, the time zone of the machine where the Change Auditor client resides will be used.

Send to a mailbox

Specifies that you want to share reports through email.

Send to a shared folder

Specifies that you want to select a shared folder to write reports to. The credentials from the Shared Folder Configuration are used to write reports to the shared folder. Ensure that the account has permissions to write to the shared folder. (The credentials are configured in the Change Auditor client under the coordinator configuration Shared Folder Configuration option.)

Do not send empty reports

When selected, a report will not be sent to email or a shard folder if it does not contain any results.

Send empty report email notification

Select this to receive an email notification for a report that ran but did not contain any results. This is only available if you have selected the send to a mailbox and the Do not send empty reports options.

To

Enter the email address of the recipients to receive the report or the shared folder to write the report.

For shared folders, the To field is automatically populated with the default shared folder path. However, you can specify a different path. You must enter a network path; a local address will not be accepted.

Reply

(Optional) Enter the email address to which reply emails are to be sent.

Cc

(Optional) Enter the email address of users who are to receive a carbon copy of the report email.

Bcc

(Optional) Enter the email address of users who are to receive a blind carbon copy of the report email.

> **i** | **NOTE:** You can enter an individual email address or distribution list in any of the email address fields. Separate multiple email addresses with a semi-colon.

Layout tab

Use the Layout tab to define the data (columns) to retrieve from the database and display in the Search Results page. From this tab, you can also define the column order, sort criteria and order, and groupings to be used to display the retrieved data.

The Layout tab contains the following tables and controls:

Retrieve data tables

The left-most tables allow you to select the event details that are to be retrieved from the database for display in the web client.

Unselected Columns table

Displays the event details that can be retrieved from the database.

Selected Columns table

Displays the event details that are being retrieved from the database. It also displays the order in which the columns will be presented in the Search Results grid.

To add a column, select the column from the Unselected Columns table and use the right arrow button (located between these two tables) to move it to the Selected Columns table.

To remove a column from display, select the column from the Selected Columns table and use the left arrow button (located between these two tables) to move it back to the Unselected Columns table.

To rearrange the order of the columns, in the Selected Columns table select the column to be moved and use the up or down arrow button (located to the right of the Selected Columns table) to move the selected column to the desired location.

To reset the column selection and arrangement back to the factory defaults, use the reset button located next to the lower right corner of the Selected Columns table.

Sort criteria table

The table to the right of the Selected Columns table defines the criteria to be used to sort the search results.

To define the sort criteria for your search results, select a column in the Selected Columns table and use the right arrow button (located to the right of the Selected Columns table) to move it to the Sort Criteria table. To specify secondary sort criteria, add the additional columns to the Sort Criteria table. Use the arrow controls to the right of this table to define the primary (first column in list) and subsequent sort criteria.

Order By

This column lists the event details selected for sorting the search results.

Direction

This column specifies the sort direction for the sort criteria:

- ASC: ascending
- DESC: descending

To change the sort direction, place your cursor in the corresponding **Direction** cell and select **Ascending** or **Descending**.

Group By

This column indicates whether the displayed information is to be grouped. (Similar to selecting a column heading in the Search Results grid and dragging it to the space above the table to group the displayed information.)

To group/ungroup data, place your cursor in the corresponding **Group By** cell and select **Yes** to group the data or **No** to remove a grouping.

To reset the settings in the Sort Criteria table back to the factory defaults, use the reset button located next to the lower right corner of the Sort Criteria table.

SQL tab

The SQL tab displays the SQL query built to run the selected search. This information is only available once a search has been created.

i | **NOTE:** The SQL tab is hidden by default. To display this tab, select the **Show SQL Tab** check box on the Searches page of the Client Settings dialog.

XML tab

The XML tab displays the XML representation of the search criteria.

i | **NOTE:** The XML tab is hidden by default. To display this tab, select the **Show XML Tab** check box on the Searches page of the Client Settings dialog.

Search Results Page

- Introduction
- Data grid view
- Timeline view

Introduction

When you run a search, a new Search Results page is added to the web client, where you can view the event records returned. As you run additional searches, they are listed with the main web pages under **Search Results** (visible when the left side menu is expanded).

The events returned as a result of a search, can be viewed in one of two views:

- Data grid view
- Timeline view

Data grid view

The Data grid view is the default view whenever a Search Results page (or Overview Drilldowns page) is opened. This view consists of the following main components:

- Search results grid: The main display area of a Search Results page that displays the events captured as a result of running a search from the Searches page.
- Event Details pane: The pane displayed across the bottom of a Search Results page that contains additional details about the event selected in the Search Results grid.

Use the tool bar buttons on the page to modify the default display, which contains the Search Results grid and Event Details pane.

Table 14. Data grid view: Tool bar buttons

Tool bar button	Description
Search Properties | **Event Details**	Click **Search Properties** to display the Search Properties tabs, replacing the Event Details pane across the bottom of the Search Results page. Click **Event Details** to redisplay the Event Details pane.
Timeline	Click to display the search results as event markers in a Timeline view instead of a list of events in the Data Grid view.
Columns	Click to display a list of columns that can be shown or hidden in the Search Results grid. Checked columns will be displayed in the grid; cleared columns will not appear in the grid.
Print	Click to print the search results.
Print to File	Click to save the search results to a csv or pdf file.
Close	Click to close the Search Results page.

Search results grid

The search results grid displays a default set of data, which can be customized by using the controls in the column headings. As on other web client pages, you can modify the sort criteria and filter the contents to be displayed (see Customize table content). In addition, the search results grid allows you to group the results by column heading in order to create an expandable view of the events.

Group data on search results grid

The grouping feature allows you to group data to create a collapsed view that can be expanded to view the individual events pertaining to that group.

To group data:

1. Click and hold on a column heading (the column heading will pop off the table) and drag it to the space above the grid. For example, use the left mouse button to click the Subsystem heading and drag that column heading to the space above the table.

2. Optionally, repeat this step to select additional headings to create a hierarchy of groupings.

   This will collapse the table and display the groupings that can be expanded to view the detailed information that applies to that group.

3. To expand a group and display the individual events listed, click on the expand properties button (right arrow) to the left of the label. Click the arrow again to collapse an expanded group.

4. To remove a grouping, select the heading and drag it back down into the table area or click the X on the group heading button.

   i | **NOTE:** Selecting the **F5** key to refresh your screen resets the data grid back to the grouping defined in the search's Layout tab, removing any groupings that have been applied.

Event Details pane

The Event Details pane provides additional details about the event selected in the grid at the top of the Search Results page. The contents of this pane depends on the type of event selected. However, all events display the following details:

Table 15. Event Details pane

Field	Description
Severity	Displays the severity level assigned to the event.
Who	Specifies the name of the user who initiated the change. If available, the display name of the user account is also displayed in parenthesis.
When	Specifies the date and time when the change occurred.
Where	Displays the name of the server where the change occurred.
Source	Displays the source of the event: • Change Auditor • ActiveRoles Server • GPOADmin **NOTE:** When the event is generated from Active Roles Server or GPOADmin, the name of the user account that initiated the event is displayed in parenthesis.
Origin	If available, displays the NetBIOS name and IP address of the workstation or server from which the event was generated. **NOTE:** When the browser is running on the IIS server and a change is made on the Administration Tasks page of the web client, the Origin is reported as ::1 (::1). This is expected because the IIS server variable value is ::1.

Table 15. Event Details pane

Field	Description
What	Displays a brief description of the change that occurred. There are three basic types of events generated that determine the 'what' information displayed: • Occurrence events (e.g., an object is created or deleted) • Change events • Delta events (e.g. DACL/SACL changes) Depending on the type of event, additional details may be displayed on this pane. See the Quest Change Auditor User Guide for a description of the additional fields that may be displayed.
Result	Indicates whether the operation mentioned in the event was successfully completed. Valid states are: • Success (Green): Indicates that the operation occurred as stated in the event. • Protected (Yellow): Indicates that the operation did not occur because the object is being protected by the Change Auditor object locking feature. • Failed (Red): Indicates that the operation did not occur due to a factor/setting outside of Change Auditor's control. • None (Gray): Indicates that the operation occurred as stated, but no results were captured for the event. Note that this state is used for most of the internal Change Auditor events.
Subsystem	Defines the subsystem, or area of monitoring, where the event occurred (e.g., Active Directory, Service, Group Policy, etc.)
Action	Defines the action associated with the selected event.
Facility	Displays the event class facility to which the event belongs.

To view the event details for an event:

1   Select an event from the Search Results grid to display the Event Details pane across the bottom of the page.

> **i** | **NOTE:** Using a mobile browser, the Event Details pane is opened in a new window.

2   To email the selected event's details, click **Email**.

This will create a new email containing a link to the Event Details pane. Enter the recipient's email address and edit the subject line if desired. Click **Send**.

3   To view the event reference guide associated with the selected event, click **Knowledge Base**.

4   To view or add comments to the selected event, click **Comments**.

In the **New Comments** text box at the bottom of the dialog, enter the comments to be associated with the selected event then click **Save**. All previously saved comments appear listed in the comments text box at the top of the dialog.

5   To disable an event, click **Disable**.

6   To run a related search, expand the **Related Search** button and select the appropriate option:

- **Who**: Select this option to run a query for all events generated by this user during the same date interval as that specified in the When tab of the selected event.

- **View Contact Card**: For events with a user object, select this option to view the contact card for the user, which includes contact information as well as a list of the groups to which this user belongs.

- **Where**: Select this option to run a query for all events captured by this agent during the same date interval as that specified in the When tab of the selected event.

- **View Resources**: Select this option to display the Resources Details pane for this server, which includes: Machine Info, Processors, Drives, Shares, Services and Exchange Mailboxes.

See the Quest Change Auditor User Guide for more information about the information displayed on this pane.

- **What**: Select this option to run a query for events captured for this event class during the same date interval as that specified in the When tab of the selected event.

- **When**: Select this option to run a query for events that occurred on this date.

- **Origin**: Select this option to run a query for events that originated from this workstation or server during the same date interval as that specified in the When tab of the selected event.

- **Object**: Select this option to run a query for events generated against this object during the same date interval as that specified in the When tab of the selected event.

  i | **NOTE:** This last option is the 'object' from the original event, such as a file or folder, a directory object, registry key, etc..

7   To restore a changed value to the previous value on a simple Active Directory object event, click the **Restore Value** button. If prompted for credentials, enter the credentials for a user with domain rights to access the selected object. (This button only appears for simple Active Directory object events, such as Add Attribute, Modify Attribute, Delete Attribute.)

i | **NOTE:** To collapse and hide the Event Details pane, click the down arrow in the divider bar between the Search Results grid and Event Details pane. To expand a collapsed Event Details pane, click the up arrow in the divider bar at the bottom of the screen.

Timeline view

The Timeline view contains event markers within an interactive timeline. The top band of the timeline contains event markers that correspond to the events returned as a result of a search. The bottom bands provide a zoomed out overview of the event markers displayed on the top band. The distribution and display of these event markers are predefined; however, these settings can be modified to meet your needs.

The Timeline view consists of the following main controls:

- Event markers
- Navigation Control panel

Use the tool bar buttons at the top of the page to return to the Data Grid view or close the Search Results page.

Table 16. Timeline view: Tool bar buttons

Tool bar button	Description
Grid	Click to display the search results in a Data Grid view instead of the Timeline view.
Close	Click to close the Search Results page.

Event markers

Event markers representing an individual event or a group of events are plotted on the timeline based on when the event actually occurred. The events associated with an event marker are controlled by the settings in the Timeline Display Settings dialog.

Each event marker contains the following components:

- Severity icon: For individual events, the colored icon represents the severity assigned to the event: red (high), yellow (medium) or green (low). For a group of events, this icon is gray.

- Event Marker label: The label attached to each event marker is determined by the group settings and date/time of an event. For an individual event, the label is the actual event class; whereas, the label for a group of events is the name of the agent where the events occurred followed by the number of events included in the group.

Event maker labels are displayed by default; however, you can clear the **Show event label** check box on the Timeline Display Settings dialog to hide all labels.

Navigation Control panel

The default settings for distributing and displaying events in the timeline can be customized by changing the display and group settings on the Timeline Display Settings dialog or by using the zoom slide bar on the Navigation Control panel.

The Navigation Control panel is located to the left of the top band in the timeline, and contains the following controls.

Table 17. Navigation Control panel: Buttons

Button	Description
⚙	Click this button to modify the settings used to define how events are to be distributed and displayed in the timeline. See Timeline Display Settings dialog for more information on the available settings.
🕐	Click this button to define how to center the event markers on the timeline, based on: • Specific date and time • Oldest event • Newest event **NOTE:** The default is the current date and time.
+	Click this button to move the zoom slide bar up to expand the event markers within a more granular time scale.
−	Click this button to move the zoom slide bar down to condense the event markers on a less granular time scale.

Timeline Display Settings dialog

The Timeline Display Settings dialog appears when you click the ⚙ button at the top of the Navigation Control panel. Use this dialog to filter or highlight the event markers in the timeline, show or hide event marker labels, and control the grouping of events.

Use the settings on this dialog to define how events are to be distributed and displayed in the Timeline view.

Filter

Use the filter field to customize the timeline to show a subset of event markers based on the text string entered.

As you enter text into the filter field, event markers that correspond to events that contain the text string in their event description will remain on the timeline; whereas, events that do not contain the text string will be cleared from the timeline.

> **NOTE:** Event markers will be cleared from both the top and bottom bands.

Highlight

Use the highlight fields to add highlighting to specific event markers within the timeline.

As you enter text into one of the highlight fields, event markers that correspond to events that contain the text string in their event description will be highlighted in the corresponding color.

> **NOTE:** Highlighting applies to event markers in both the top and bottom bands.

Show event label

This check box is selected by default indicating that event marker labels are to be displayed in the top band of the timeline.

Clear this check box to turn off the rendering of event labels in the timeline.

Group same events that occur on the same agent within *nn* minutes

This check box is selected by default, meaning that if the same event occurs on the same agent within five minutes of each other, these events are to be grouped together in the same event marker on the timeline. Using this setting, you are seeing 'event class' event markers.

> **i** | **NOTE:** By clearing this group setting, each event marker now represents a group of events on the same agent.

Group all events that occur on the same agent within *nn* minutes

This check box is selected by default, meaning that all events that occur on the same agent within 30 minutes of each other are to be grouped together in the same event marker on the timeline. Using this setting, you are seeing 'agent' event markers.

> **i** | **NOTE:** By clearing only this group setting, each event marker now represents an 'event class'. By clearing both group settings, each event marker represents a single event.

Navigate timeline

Adjust time scale

Use the zoom bar controls on the Navigation Control panel to adjust the time scale for the timeline and redistribute your event markers according to the new scale. By default, the timeline displays the least granular time scale (days); however, by sliding the control up the zoom bar or clicking the ⊞ button you can redistribute your event markers at hour increments.

Scroll timeline

Use one of the following methods to scroll through the event markers in the displayed timeline:

- Drag your mouse pointer horizontally to adjust the timeline view. You can use this method on any of the bands within the timeline to view an earlier or later date/time.

- Use the arrow controls to the far right and left of the screen to scroll by page. That is, click the right arrow to view the next page and click the left arrow to view the previous page.

- Double-click an area on one of the bottom banks to go to the date/time represented in the selected area.

In addition, when the timeline contains more event markers than what can be displayed vertically, scroll bars are added allowing you to scroll up and down to view these additional event markers for the displayed time interval.

Center timeline

By default, the current date and time is used to center the event markers on the timeline.

To modify the center of the timeline:

1 Click the 🕐 button on the Navigation Control panel.

2 From the dialog displayed, select one of the following options:

   - **This date**: Select this option and use the calendar and clock controls to set the date and time to be used. (Default)

- **Oldest event**
- **Newest event**

3 Click outside the dialog to save your selection and adjust the center of the timeline.

View event details in Timeline view

Hovering your mouse pointer over an event marker displays an event tool tip box which displays a list of the event class groupings, with number of events in parentheses, associated with the selected event marker.

Clicking an event marker displays an event summary pop-up box that lists more details about the event class groupings associated with the selected event marker.

The pop-up box displays the following information for each event class grouping associated with the selected event marker:

- Event class with number of occurrences in parenthesis.

- Severity (colored icon in upper right corner)

- Event message, which is a hypertext link which when selected displays the Search Results grid and Event Details pane for the event.

- Date/time event occurred on agent. If the event marker contains multiple occurrences, clicking the arrow control adds a list of dates/times when the event occurred. In some cases, clicking the arrow control adds a scroll bar allowing you to scroll through these additional dates/times.

  These additional dates/times are also hypertext links which when selected display the Search Results grid and Event Details pane for that occurrence of the event.

To close the pop-up box, click the close button in the upper right corner or click outside the pop-up box.

Administration Tasks Page

- Introduction
- Administration Task lists
- Managing templates

Introduction

The Administration Tasks page allows you to perform a variety of administration tasks based on the Change Auditor licenses that are applied. Click the **Administration Tasks** link in the expanded left pane or click the Administration Tasks icon to display the Administration Tasks page, which consists of a navigation pane to the left and information pages to the right.

> **i** | **NOTE:** Authorization to use the administration tasks on the Administration Tasks page is defined using the Application User Interface page. If you are denied access to the tasks on this page, refer to Application User Interface Authorization page.

The Administration Tasks page navigation pane is divided into different task lists: Configuration, Auditing and Protection. Click a task button from the bottom of the navigation pane to display a task list. Then select a task from the displayed task list to display the appropriate information page, from which you can perform the corresponding administrative task.

Administration Task lists

The following table lists the navigation pane's task lists and a brief description of the administrative tasks that can be performed. Many of the tasks listed require a specific Change Auditor license, which is indicated by the following codes in the last column of the table:

- Any - does not require a specific license; available with any license
- CAAD - Change Auditor for Active Directory
- CAEX - Change Auditor for Exchange
- CAFS - Change Auditor for Windows File Servers
- CASQL - Change Auditor for SQL Server
- CAAD-Q - Change Auditor for Active Directory Queries
- CAEMC - Change Auditor for EMC
- CANA - Change Auditor for NetApp
- CAFFS- Change Auditor for Fluid File System

- CASP - Change Auditor for SharePoint

i | **NOTE:** You are not prevented from performing any of the administration tasks on the Administration Tasks page; however, associated events are not captured and associated protection does not occur unless the proper license is applied.

To view the licenses currently applied, click the information icon in the upper right corner of the heading bar and open the Licenses tab.

For more detailed information on how to perform an administrative task or a description of the page that is displayed, refer to the appropriate chapter in the different Change Auditor user guides.

Table 18. Administration Task tab: Task descriptions

Task List/Task	Description	License
Configuration		
The following tasks are available in the Configuration task list:		
Agent	Define and assign agent configurations.	Any
	See Agent Configuration page, and for additional information refer to the Quest Change Auditor User Guide.	
Coordinator	Enable email alert notifications/reports, configure mail server to be used for SMTP alerting/reporting, define group membership expansion, and modify agent heartbeat check interval.	Any
	See Coordinator Configuration page, and for additional information refer to the Quest Change Auditor User Guide.	
Purge Jobs	Define and schedule purge jobs for deleting events from the production database.	Any
	See Purge and archive jobs, and for additional information refer to the Quest Change Auditor User Guide.	
Report Layouts	Define report layout templates which contain the header/footer information to be used in reports.	Any
	See Report Layouts page, and for additional information refer to the Quest Change Auditor User Guide.	
Application User Interface	Define who is authorized to use the various Change Auditor client features.	Any
	In addition you can define who is authorized to view the Active Directory and Group Policy protection tasks in Change Auditor.	
	See Application User Interface Authorization page, and for additional information refer to the Quest Change Auditor User Guide	
Auditing		
The Auditing task list is divided into separate lists that identify configuration tasks, forest-level tasks that are globally applied, tasks that define auditing for different applications, server-level tasks that must be assigned to an agent configuration, and tasks that define NAS device auditing.		
Configuration		
Use the tasks under this heading to configure the events to be captured by Change Auditor and to define accounts that are to be excluded from auditing.		
Audit Events	Enable/disable event auditing and modify an event's severity level or description.	Any
	See Audit Events, and for additional information refer to the Quest Change Auditor User Guide.	
Excluded Accounts	Create Excluded Accounts templates to define individual accounts that are to be excluded from Change Auditor auditing.	Any
	See Excluded Accounts auditing, and for additional information refer to the Quest Change Auditor User Guide.	

Table 18. Administration Task tab: Task descriptions

Task List/Task	Description	License
Forest		
Use the tasks under this heading to define custom auditing definitions for your Active Directory forest.		
Active Directory	Define custom Active Directory object class auditing.	CAAD
	See Active Directory auditing, and for additional information refer to the Quest Change Auditor for Active Directory User Guide.	
Attributes	Define custom Active Directory attribute auditing.	CAAD
	See Active Directory auditing, and for additional information refer to the Quest Change Auditor for Active Directory User Guide.	
Member of Group	Define a Member of Group auditing list to specify the users to be audited based on their group membership.	CAAD
	See Member of Group Auditing page, and for additional information refer to the Quest Change Auditor for Active Directory User Guide.	
AD Query	Define the Active Directory containers that are to be included or excluded from AD query auditing.	CAAD-Q
	See AD Query Auditing page, and for additional information refer to the Quest Change Auditor for Active Directory Queries User Guide.	
ADAM (AD LDS)	Define custom ADAM (AD LDS) object auditing.	CAAD
	See ADAM (AD LDS) Auditing page, and for additional information refer to the Quest Change Auditor for Active Directory User Guide.	
Attributes	Define custom ADAM (AD LDS) attribute auditing.	CAAD
	See ADAM (AD LDS) Attribute Auditing page, and for additional information refer to the Quest Change Auditor for Active Directory User Guide.	
Applications		
Use the tasks under this heading to define auditing for different types of applications within your environment.		
Exchange Mailbox	Define an Exchange Mailbox auditing list to specify which directory object's mailbox activities are to be audited by Change Auditor for Exchange.	CAEX
	See Exchange Mailbox auditing, and for additional information refer to the Quest Change Auditor for Exchange User Guide.	
SQL	Create SQL Auditing templates to define the SQL instances and operations that are to be audited.	CASQL
	See SQL auditing, and for additional information refer to the *SQL auditing for* Quest Change Auditor SQL Server User Guide.	
VMware	Create VMware Auditing templates to define the VMware hosts to be audited and the Change Auditor agent to be used to audit these hosts.	Any
	See VMware auditing, and for additional information refer to the Quest Change Auditor for VMware User Guide.	
SharePoint	Create SharePoint Auditing templates to define the SharePoint farm to be audited and the Change Auditor agent to be used to audit this farm.	CASP
	See SharePoint auditing, and for additional information refer to the Quest Change Auditor for SharePoint User Guide.	

Table 18. Administration Task tab: Task descriptions

Task List/Task	Description	License
Server		
Use the tasks under this heading to create auditing templates that can then be assigned to agent configurations to enable custom server-level auditing.		
File System	Create File System Auditing templates to define the files/folders that are to be audited. See File System auditing, and for additional information refer to the Quest Change Auditor for Windows File Servers User Guide.	CAFS
Registry	Create Registry Auditing templates to define the registry keys and events that are to be audited. See Registry auditing, and for additional information refer to the Quest Change Auditor User Guide.	Any
Services	Create Service Auditing templates to specify the system services that are to be audited. See Services auditing, and for additional information refer to the Quest Change Auditor User Guide.	Any
NAS		
Use the tasks under this heading to create auditing templates for NAS devices.		
EMC	Create a separate EMC Auditing template for each CIFS file access protocol to be audited by Change Auditor, defining the EMC file server (CIFS), auditing scope and agent(s) that are to receive the EMC events. See EMC auditing, and for additional information refer to the Quest Change Auditor for EMC User Guide.	CAEMC
NetApp	Create a separate NetApp Auditing template for each NetApp filer to be audited by Change Auditor, defining the NetApp filer, the auditing scope, and the agents that are to receive the NetApp events. See NetApp auditing, and for additional information refer to the Quest Change Auditor for NetApp User Guide.	CANA
FluidFS	Create a separate FluidFS auditing template for each FluidFS cluster to be audited by Change Auditor, defining the cluster, the auditing scope, and the agents that are to receive the events. See Fluid File System (FluidFS) auditing, and for additional information refer to the Quest Change Auditor for Fluid File System User Guide.	CAFFS
Protection		
The Protection task list is divided into separate task lists as well: one for forest-level tasks that are globally applied, one for tasks that define protection for applications, and another for server-level tasks that must be assigned to an agent configuration.		
Forest		
Use the tasks under this heading to define global protection definitions for your Active Directory forest.		
Active Directory	Create Active Directory Protection templates to define critical Active Directory objects that are to be protected against unauthorized modifications. See Active Directory object protection, and for additional information refer to the Quest Change Auditor for Active Directory User Guide.	CAAD

Table 18. Administration Task tab: Task descriptions

Task List/Task	Description	License
ADAM (AD LDS)	Create ADAM (AD LDS) Protection templates to define critical ADAM objects that are to be protected against unauthorized modifications. See ADAM (AD LDS) object protection, and for additional information refer to the Quest Change Auditor for Active Directory User Guide.	CAAD
Group Policy	Create Group Policy Protection templates to define critical Group Policy objects that are to be protected against unauthorized modifications. See Group Policy object protection, and for additional information refer to the Quest Change Auditor for Active Directory User Guide.	CAAD
Applications		
Use the task under this heading to define global protection for your Exchange Mailbox application.		
Exchange Mailbox	Create Exchange Mailbox Protection templates to define critical Exchange Mailboxes that are to be protected against unauthorized modifications. See Exchange Mailbox protection, and for additional information refer to the Quest Change Auditor for Exchange User Guide.	CAEX
Server		
Use the task under this heading to create protection templates that can then be assigned to agent configurations to enable server-level protection.		
File System	Create File System Protection templates to define critical files/folders that are to be protected against unauthorized modifications. See File System protection, and for additional information refer to the Quest Change Auditor for Windows File Servers User Guide.	CAFS

Managing templates

After a template has been created on a task page, it can be modified, copied, disabled, re-enabled and deleted. The following procedures apply to previously created templates.

- Modify a template
- Copy a template
- Disable/enable a template or item in a template
- Delete a template

ℹ **IMPORTANT:** To enable various custom auditing and protection features, you are required to assign templates to an agent's configuration. The custom auditing and protection features that require custom templates to be assigned to an agent's configuration are:

- File System auditing
- Registry auditing
- Service auditing
- SQL Server auditing
- Excluded Accounts auditing
- File System protection

The Agent Configuration page explains how to apply the above templates using the web client. For additional information, refer to the Quest Change Auditor User Guide.

The NetApp, EMC, FluidFS, SharePoint, and VMware auditing templates define which agents are used to capture events; however, these templates do not use the agent configurations from the Agent Configuration page. See Templates with defined agents for more information.

Modify a template

To modify a template:

1   On the appropriate task page, select the template to be modified and click **Edit**.

This displays the template's wizard where you can make modifications to the selected template.

2   Click **Finish** to save your changes and return to the task page.

Copy a template

ℹ **NOTE:** The following auditing templates may be copied:

- SQL Server auditing
- File System auditing
- Registry auditing
- Services auditing

To copy a template:

    1   On the appropriate task page, select the template to be copied and click **Copy**.

        An identical template will be added as Copy of *<Original Template Name>*.

    2   Select the new template and click **Edit** to open the auditing wizard to rename and edit the template.

Disable/enable a template or item in a template

Templates are automatically enabled when they are created. The disable feature allows you to temporarily stop auditing/protection without having to remove the template.

To disable/enable a template:

    1   On the appropriate task page, select the template to be disabled and click **Disable**.

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

    2   To re-enable the template, use the **Enable** option.

To disable/enable an item in a template:

    1   On the appropriate task page, select the item to be disabled and click **Disable**.

        The entry in the **Status** column for the item changes to 'Disabled'.

    2   To re-enable the auditing or protection of an item, use the **Enable** option.

    i | **NOTE:** On some templates, if you disable all of the items, the template itself will become disabled. Similarly, when you re-enable the only item in the template, the template will automatically be re-enabled.

Delete a template

To delete a template:

    1   On the appropriate task page, select the template to delete and click **Delete** | **Delete Template**.

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

To delete an item from a template:

    1   On the appropriate task page, select the item to deleted from a template and click **Delete** | **Delete *<nn>***.

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

    i | **NOTE:** In some cases, when you delete the last item in a template, the entire template will be deleted.

Configuration Tasks (Administration Tasks Page)

- Introduction
- Agent Configuration page
- Coordinator Configuration page
- Purge and archive jobs
- Report Layouts page
- Application User Interface Authorization page

Introduction

The following sections describe the pages available through the Configuration task list of the Administration Task page and the tasks that can be performed on each of these pages. These pages allow you to define and assign agent configurations, enable email alerting and reporting, enable group membership expansion, define database purging, design templates for reports and authorize who is able to perform the different Change Auditor operations. For a full description of all options and fields available on these Configuration Tasks pages, refer to the Quest Change Auditor User Guide.

Agent Configuration page

Use the Agent Configuration page to define and assign agent configurations. The Agent Configuration page is displayed when **Agent** in the Configuration task list is selected in the navigation pane of the Administration Tasks page.

Table 19. Agent Configuration page: Tool bar buttons

Tool bar button	Description
Columns	Use to display different fields on the Agent Configuration page.
Configurations	Use to display the Configuration Setup dialog to add, edit or delete agent configuration definitions. See Defining and assigning agent configurations.
Assign	Use to assign an agent configuration to the selected agents.
Default All	Use to reset all agent configurations back to the default configuration.
Refresh Configuration	Use to retrieve the current agent configuration assignments.
Event Logging	Use to enable/disable event logging. See Enable event logging.

Defining and assigning agent configurations

To enable various custom auditing and protection features you are required to assign templates to an agent's configuration. The custom auditing and protection features that require custom templates to be assigned to an agent's configuration are:

- File System auditing
- Registry auditing
- Service auditing
- SQL Server auditing
- Excluded Accounts auditing
- File System protection

i | **NOTE:** The NetApp, EMC, FluidFS, SharePoint, and VMware auditing templates define which agents are used to capture events; however, these templates do not use the agent configurations as described below. See Templates with defined agents for more information.

Define agent configurations

To define a new agent configuration:

1   Open the Administration Tasks page.

2   Click **Configuration**.

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

4   From the Agent Configuration page, click **Configurations**.

The Configuration Setup dialog is displayed, where the top pane contains a drop-down list of configuration definitions available as well as the means for creating a new configuration. To view the Configurations list, click the arrow control to the far right of the tool bar buttons. After selecting a configuration from the list, the cell updates to display the name of the currently selected configuration.

5   Click **Add** to create a new definition or click **Copy** to duplicate the configuration displayed in the cell.

This adds a new configuration to the list, allowing you to name the new configuration, specify the system settings and assign auditing and protection templates to the configuration.

6   With the new/copied configuration displayed in the cell, enter the name for the new agent configuration in the **Configuration Name** field.

7 Use the tabs on the bottom pane to assign templates or view/modify agent settings.

Table 20. Configuration Setup dialog

Tab	Description	Procedure
Template	Use to add templates to selected agent configuration	1 Select the corresponding check box in the **Assigned** column 2 Click **Apply** to save your selection.
System Settings	Use to define how agents are to process events	1 Modify the following settings: ▪ Polling Interval ▪ Forwarding Interval ▪ Retry Interval ▪ Agent Load Threshold ▪ Max events per connection ▪ Allowed time for connection 2 Click **Apply** to save your selection.
File System	Use to define how to process duplicate file system events **NOTE:** Applies to Change Auditor for Windows File Servers, Change Auditor for EMC, or Change Auditor for NetApp events	1 Modify the following settings: ▪ Discard duplicates that occur within *nn* seconds ▪ Audit all configured, including duplicates (Not recommended) 2 Click **Apply** to save your selection.
AD Query	Use to optimize the Active Directory auditing process **NOTE:** Applies to Change Auditor for Active Directory Queries	1 Modify the following settings: ▪ Discard query results less than *nn* records ▪ Discard queries taking less than *nn* milliseconds ▪ Discard duplicate queries that occur within *nn* minutes ▪ AD Query auditing enabled 2 Click **Apply** to save your selection.
Exchange	Use to define how to handle duplicate folder events **NOTE:** Applies to Change Auditor for Exchange	1 Modify the following setting: ▪ Discard duplicates that occur within *nn* seconds 2 Click **Apply** to save your selection.
VMware	Use to define how often the agent is to poll VMware for new VMware events	1 Modify the following setting: ▪ Polling Interval 2 Click **Apply** to save your selection.

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

Assign agent configurations to agents

Once agent configurations are defined they can be assigned to one or more installed agents. Use the Agent Configuration page to assign agent configurations to agents.

To assign a configuration to an agent from the Agent Configuration page:

1 On the Agent Configuration page, select one or more agents from the agent list and click **Assign**.

2   On the Agent Assignment dialog, select the configuration definition to be assigned to the selected agents and click **OK**.

3   Back on the Agent Configuration page, the agent configuration assignment will be updated in the Configuration column.

4   Select the agents assigned to the agent configuration and click **Refresh Configuration** to ensure that the assigned agents are using the latest agent configuration.

> **i** | **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.

Templates with defined agents

The following auditing templates define the agents to be used to capture events:

- NetApp auditing
- EMC auditing
- FluidFS auditing
- SharePoint auditing
- VMware auditing

To enable the auditing defined in these templates, you must refresh the selected agent's configuration after creating the template.

Refreshing an agent's configuration to enable a newly assigned auditing template:

1   Open the Administration Tasks page.

2   Click **Configuration**.

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

4   Select the agents assigned to the auditing template and click **Refresh Configuration** to ensure the agent is using the latest configuration.

> **i** | **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.

Enable event logging

Using the Agent Configuration page you can also enable the event logging feature which writes Change Auditor events locally to a Windows event log. These event logs can then be collected using InTrust to satisfy long-term storage requirements.

> **i** | **NOTE:** Event logging must be enabled for Change Auditor's events to be available in InTrust.

NOTE: This is a global setting and applies to all agents. However, keep the following in mind when defining custom auditing:

- Disabling Change Auditor events does NOT impact event logging.
- Excluding accounts from auditing does NOT impact event logging with the exception of Exchange. That is, if an Exchange Mailbox account is set to exclude ALL mailbox events, then these events will also be excluded from the event log.
- Event logging is disabled by default for the following. When enabled, only configured activities are sent to the event log.
    - Registry events
    - Service events
    - SharePoint events
    - FluidFS events
    - NetApp events
    - EMC events
    - SQL Data Level events
    - SQL Server events
    - File System events
- For Active Directory events, event logging is disabled by default. When enabled, all Active Directory activity is sent to the event log.
- For ADAM (AD LDS) events, event logging is disabled by default. When enabled, all ADAM activity is sent to the event log.
- For Exchange mailbox events, event logging is disabled by default. When enabled, only configured Exchange Mailbox activities are sent to the event log. Office 365 Exchange Online events are NOT logged to this event log.
- For AD Query events, event logging is disabled by default. When enabled, all Active Directory queries, except those specified in the Excluded AD Query list are sent to the event log. When enabling AD Query event logging, keep in mind that AD Query events could be of very high volume.
- For Skype for Business events, event logging is disabled by default. When enabled, all Skype for Business events are sent to the event log.

To enable event logging:

1 Open the Administration Tasks page.

2 From the left pane, select **Agent** (under the Configuration task list) to display the Agent Configuration page.

3 Click **Event Logging**.

4 On the Event Logging dialog, select the type of event logging to be enabled:
- Active Directory
- ADAM (AD LDS)
- Exchange
- File System
- SQL
- SQL Data Level
- EMC
- FluidFS
- AD Query
- Registry
- Service

- Local Account

- Change Auditor

- NetApp

- SharePoint

- Skype for Business

ℹ **NOTE:** If an option is disabled, this indicates that you do not have the corresponding component licensed. For example, if the SharePoint check box is disabled, you do not have a Change Auditor for SharePoint license.

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

Coordinator Configuration page

The Coordinator Configuration page is displayed when **Coordinator** is selected from the Configuration task list in the navigation pane of the Administration Tasks page.

This page consists of the following panes:

- **SMTP Configuration** - for enabling and configuring email alerting and reporting.

- **Group Membership Expansion** - for defining the schedule for expanding nested membership of Active Directory groups that are referenced in searches (Who search criteria) or groups that are defined in the Member of Group auditing feature.

- **Agent Heartbeat Check** - for specifying how long the coordinator service is to wait before an agent that is not sending updates will be marked as 'inactive'. By default, the agent will be marked inactive after 30 minutes and the coordinator service will not attempt to restart the agent service.

Table 21. Coordinator Configuration page: Tool bar buttons

Tool bar button	Description
Apply Changes	Use to save your coordinator configuration settings.
Test SMTP	Use to generate a test email based on the configuration information entered in the SMTP Configuration pane.
Test SNMP	Use to generate a test SNMP trap based on the configuration information entered in the SMTP Configuration pane.

Configure email alert notifications/reports

To dispatch configuration change alerts or reports through email (SMTP), you must enable email notification on the Coordinator Configuration page.

ℹ **NOTE:** The settings set on this page are global settings and apply to all email alert notifications and reports.

For alerts, you can override the reply to, alert subject, signature and body content for individual search queries using the settings on the Alert tab (Search Properties tabs).

For reports, you can override the reply to address for individual search queries using the Report tab (Search Properties tabs).

ℹ **NOTE:** Change Auditor sends alerts through a single SMTP (email) relay even when multiple coordinators are configured. That is, all coordinators will use the same mail server for sending alert notifications and reports.

To enable and configure email notifications/reports:

1 Open the Administration Tasks page.

2 Click **Configuration**.

3   Select **Coordinator** in the Configuration task list to open the Coordinator Configuration page.

4   On the SMTP Configuration pane, select the **Enable SMTP for Alerts** option to enable email alert notifications and reporting. Checking this option activates the remaining fields on this page to define the mail server to be used.

Enter the following information:

- **Mail Server**

- **From Address**

  i   **NOTE:** Use the browse button to the right of the **From Address** field to launch the Select Exchange Users dialog.

  On the Active Directory tab, use the Browse or Search page to locate and select an Active Directory user

  If the Exchange Host information is entered at the bottom of the SMTP Configuration pane, an Exchange tab is added to this dialog. On this tab, enter a string at least three characters long in the **Find** field and click **Search** to lookup and select an Exchange user.

- **Reply To**

  i   **NOTE:** Use the button to the right of the **Reply To** field to launch the Select Exchange Users dialog.

  On the Active Directory tab, use the Browse or Search page to locate and select an Active Directory user.

  If the Exchange Host information is entered at the bottom of the SMTP Configuration pane, an Exchange tab is added to this dialog. On this tab, enter a string at least three characters long in the **Find** field and click **Search** to lookup and select an Exchange user.

- **Alert Subject**

  i   **NOTE:** Use the button to the right of the **Alert Subject** field to insert a variable into the subject line or to reset it back to the default content.

5   Select the appropriate option to have the email notification/report sent in plain text format (default) or HTML format.

6   Optionally, click **Configure Body** to open the Alert Body Configuration dialog where you can define the content of the main body, the event details and the signature to be included in your alert emails. After configuring the alert body, click **OK** to return to the Coordinator Configuration page.

  i   **NOTE:** The Alert Body Configuration settings do not apply to email reports. To define the content (columns) to be included in a report, use the Layout tab. In addition, you can use the Report Layouts page (Administration Tasks page) to create customized report layout template(s) defining the header and footer information to be used in your reports.

7   If the specified mail server requires authentication, select the **My Server Requires Authentication** check box and enter the account credentials to be used.

  i   **NOTE:** Use the button to the right of the **Account Name** field to launch the Select User dialog (Directory object picker). From this dialog, use the Browse or Search page to locate and select a user.

8   (Optional) Enter the Exchange host information as described below:

- **Exchange Host -** Enter the internet host name of your Exchange mail server. Use the field to the far right of the **Exchange Host** field to specify the Exchange version for your Exchange host.

- **Email -** Enter your full email address.

- **My Host Requires Authentication -** Select this check box if the Exchange host requires authentication and enter the **Account Name** and **Password** used to log into your email account.

  i   **NOTE:** Use the button to the right of the **Account Name** field to launch the Select User dialog (Directory object picker). From this dialog, use the Browse or Search page to locate and select a user.

Configuring the Exchange host allows you to lookup email recipients using the Exchange GAL or Active Directory. That is, when you select a browse button to lookup an email recipient from the top part of the SMTP Configuration pane, Alert Custom Email dialog or Report tab, the Select Exchange User dialog appears which contains an Exchange tab where you can enter a partial name to lookup users from the Exchange GAL in addition to the Active Directory tab (directory object picker).

9   Click **Test SMTP** to test the mail server configuration.

10 Once the mail server configuration is verified, click **Apply Changes** to save the configuration.

Now that SMTP alerting/reporting is enabled and configured, you can enable email alert notifications for individual search definitions using the Alert tab (Search Properties tabs) and/or reporting for individual search definitions using the Report tab (Search Properties tabs).

Customize alert email content

In addition to the customizable fields (Reply To, Alert Subject and Signature) on the Coordinator Configuration dialog, you can use the **Configure Body** button to define the content to be used in the main body of your alert emails as well as the event details to be included.

ℹ | **NOTE:** When accessed through the Coordinator Configuration page, these settings will apply globally to all alert emails. However, if accessed through the Alert tab, these settings will apply to the selected alert only.

ℹ | **NOTE:** The Alert Body Configuration settings do not apply to email reports. To define the content (columns) to be included in a report, use the Layout tab. In addition, you can use the Report Layouts page (Administration Tasks page) to create customized report layout templates defining the header and footer information to be used in your reports.

To customize email content:

1   Click **Configure Body** to display the Alert Body Configuration dialog.

2   On the Alert Body Configuration dialog, select the appropriate option (at the bottom of the dialog) to edit either the **Plain Text** (default) or the **HTML** representation of the alert emails. Use the tabbed pages to define the content of alert emails as described below.

Table 22. Alert Body Configuration dialog

Tab	Description	Procedure
Preview	View a sample email	1 First use the other tabbed pages to enter the body content and define the event details and signature line to be included. 2 Open the **Preview** tab to view a sample email using your defined format and content.
Main Body	Enter the text to be included and define overall layout of the alert body	Rearrange the entries, remove entries, modify/add text, or add variables. **NOTE:** The event details defined in the Event Details tab are placed in the Main Body pane using the following tag: %EVENT_DETAILS%. Do not remove this tag from the Main Body tab if you want to include the event details in the alert emails. *To add a variable:* 1 Select the **Show Variables** check box to display the variables that can be added to the main body of your email. 2 Place your cursor in the location where you want to insert a variable, then double-click the variable from the variable list.

Table 22. Alert Body Configuration dialog

Tab	Description	Procedure
Event Details	Specify the event details to be included	Rearrange the entries, remove entries, modify/add text, or add variables.
		NOTE: Do NOT modify the text surrounded by percent signs (for example, %USERNAME%). These are tags which represent actual data retrieved from the Change Auditor event that triggered the alert. See the *Change Auditor User Guide* for more information on these tags and the data retrieved by each.
		To add a variable:
		1 Select the **Show Variables** check box to display a list of the variables that can be added to the event details of your alert email.
		2 Place your cursor in the location where you want to insert a variable, then double-click the variable from the variable list.
Signature	Define the content of the signature line to be used in alert emails	Enter the text to be used in the signature line of alert emails.

3 Once defined, click **OK** to save your settings and close the Alert Body Configuration dialog.

> **NOTE:** Click the **Restore to Default** button to revert back to the default email content and format.

Add groups to Membership Expansion list

By default, the **Expand groups that are referenced in existing queries and selected groups** option is selected on the group Membership Expansion pane of the Coordinator Configuration page. With the option selected, you can add groups to the Group Membership Expansion list as described below:

To add groups to Membership Expansion list:

1 Click **Add** to display the Add Groups dialog.

2 Use the Browse or Search page to locate and select a group to be added to this list. Once a group is selected, click **Add** to add it to the selection list at the bottom of the dialog.

   Repeat this step to add each additional group.

3 Once you have selected all the groups to be added, click **OK** to save your selection.

   The specified groups will now be listed in the Group Membership Expansion list back on the Coordinator Configuration page.

4 Back on the Coordinator Configuration page, click **Apply Changes** to apply your changes regarding group membership expansion.

Disconnect client after 30 minutes of inactivity

Enabling this option will force all clients to disconnect from the coordinator after 30 minutes of inactivity. If this is not selected, the option to disconnect after 30 minutes of inactivity can be selected by users when they log on to the client.

Purge and archive jobs

Change Auditor provides several options that allow you to schedule both the purging of events from your database and archiving older data to an archive database. Automating database cleanup allows you to keep critical and relevant data online and current while eliminating or archiving events that are no longer required. This not only prevents your database from growing in size, but it increases overall operational efficiency by speeding up searches and data retrieval from the database.

Using the purge options, you can define and schedule jobs that will eliminate events from the database based on the following criteria:

- All events older than a specific number of days.
- Selected events based on:
    - Who - purge events generated by a specific user, computer or group.
    - What - purge events based on subsystem, event class, object class, severity or results.
    - Where - purge events captured by a specific agent, domain or site.
    - Origin - purge events originating from a specific workstation or server.

Using the archive options, you can select to create a yearly archive database for older events that are no longer required to be represented in your reports.

Job type	Description
Purge	This deletes events from the production database. You can create and run multiple purge jobs.
	When scheduling a purge job, you can choose a batch limit. This limit tells the job how many events to delete from the production database before pausing and running another job. Choosing too large of a batch limit may slow your purge jobs down. If you find that they are slow reduce the batch limit.
Archive	This moves events from the production database to an archive database (on the same database server). The archive process removes the events from the production database during the move. Archive events do not need to be purged separately. You can only create and run one "archive" job or one "purge and archive" job.
	When scheduling an archive job for the first time it may take a long time to complete (depending on how many years of data you are asking to be archived). Batch limit does not apply to an archive type job.
	When running an archive job, you need to pay attention to disk space growth on the SQL server.
Purge and archive	This deletes events (purge job) from the production database, then immediately performs an archive job to move the remaining records in the time period specified for the job from the production database to an archive database. You can only create and run one "purge and archive" job or one "archive" job.
	If you select a batch limit, it will only apply to the purging portion of the job. When the batch limit is reached, the job will immediately run again ensuring this job type runs to completion before the archive job begins.

You will also see information regarding the status of reach job including:

- When the job was run.
- The duration of the job.
- The number of events processed.
- The coordinator involved in the process.

- Informational messages as to the status if the job:

  Immediately continuing job: Displays when the purge portion of a 'purge and archive' job continues.

  Archive database not found. Recreating archive database: Displays if an archive database has been moved or deleted.

  Starting job: Displays when the purge, archive, or purge and archive job is beginning.

  Successfully finished job: Displays when the purge and archive, purge, or archive job is finished.

  New archive database created: Displays when the new archive database has been created for the calendar year.

  Events archived: Displays the progression of the number of events being archived.

  Total events archived: Displays the total number of archived events when archiving is finished.

  Continue purge job: Displays when re-queued purge jobs run again.

Planning your jobs

Planning your jobs before scheduling them will help ensure they run as expected. Keep in mind, all jobs can take a significant time to run depending on the amount of data in your environment.

Scheduling a job

When scheduling your jobs, consider the following:

- Only one job can run at a time.

- Only one archive type job (archive only, purge/archive) can exist. However, multiple purge only jobs can be scheduled.

- Purge only jobs run until they hit the batch limit. When the batch limit is encountered the job pauses (runs again later) to give another job a chance to run. Archive type jobs will not pause to give other jobs the opportunity to run until they are complete.

- If you have multiple coordinators, only one coordinator will run job.

- Use "purge and archive" job to ensure deletion of unwanted events completes before archiving begins.

- The first time the job runs it may be working with a large amount of data and therefore may take a significant amount of time to run.

- Quest recommends that you run jobs frequently so that they are working with less data and complete faster. Start with one job to see how long it takes to complete, then add more jobs as needed.

- If an archiving job is created to archive large amounts of data over multiple calendar years, it may take a significant amount of time to finish. If you have multiple calendar years of data to archive, select to archive the oldest calendar year first. When the first archive job finishes, update the job settings to archive the next calendar year and so on until all the data has been archived.

- Enable notification on the purge and archive internal events to monitor job performance.

When multiple jobs types are scheduled to run close together the following behavior will occur:

- A list of jobs is created and ordered by next run time. If two jobs have the same run time the archive type will run first.Multiple "Purge" jobs will be executed in based on the next run time order.

  i Because of this the "purge" jobs may not complete before the "archive" or "purge and archive" jobs run if you do not plan properly.

- The "purge" job type runs until the batch limit is reached (batch limit is the total number of events to delete) and then pauses to give another "purge" job a chance to run.

During a job

During a purge and/or archive job, consider the following:

- Use internal events to monitor job performance.
- Monitor disk space on the SQL server while archiving is in progress. (No Shrink is performed)

Post job considerations

After the purge and/or archive job completes, consider the following:

- The physical database size is not changed. (Shrink operation is not performed). Once the archive database has been created, you should perform a database cleanup (shrink) on the production database as required to free up disk space.

  For information on how to perform a database shrink, see https://msdn.microsoft.com/en-us/library/ms189035.aspx.

- Multiple archive databases may be created (1 database per archived year).

- Archive databases for previous years can be detached and moved to a backup storage if needed.

Purge and Archive jobs page

The Purge and Archive page is displayed when **Purge and Archive** is selected from the Configuration task list in the navigation pane of the Administration Tasks page. From here you can specify the settings for the purge and archive jobs.

Once a job is defined, the page displays the following details about each job:

Table 23. Purge and Archive page: Field descriptions

Column	Description
Job Name	Displays the name assigned to the job when it was created using the Purge and Archive wizard.
Last Run	Displays the date and time the job last ran.
	NOTE: Based on the client's current local date and time. The format used to display this date and time is determined by the local computer's regional and language setting.
Next Run	Displays the date and time the job is scheduled to run next.
	NOTE: Based on the client's current local date and time. The format used to display this date and time is determined by the local computer's regional and language setting.
Status	Indicates whether the job is enabled or disabled.
Schedule	Displays the schedule defined for running the job.

Table 24. Purge Jobs page: Tool bar buttons

Tool bar button	Description
Add	Use to open the Purge and Archive Job wizard to define a scheduled purge job.
Edit	Use to open the Purge and Archive job wizard to modify the selected purge job.
Enable	Use to enable the selected purge or archive job.
Disable	Use to disable the selected purge or archive job.
Delete	Use to delete the selected purge or archive job.

Before scheduling a job, ensure that you have reviewed the best practice information in Planning your jobs.

> **!** **CAUTION: Carefully review your current jobs before creating a new job or altering an existing job, as it is possible to create purge and archive conflicts.**

> **i** **NOTE:** If you have specific purge jobs that you want to complete before a scheduled archive, ensure that you leave enough time between the purge only jobs and the archive job.

To schedule a database purge and/or archive job:

1 Open the Administration Tasks page.

2 Click **Configuration**.

3 Select **Purge and Archive** in the Configuration task list to open the Purge and Archive Jobs page.

4 Click **Add** to open the Purge Job wizard.

5 Begin by entering a descriptive name for the job.

6 Select the data that you want to purge and/or archive. The default is to process events older than 90 days.

> **i** **NOTE:** Jobs created in previous versions will have the process time converted from weeks/months/quarters/years to the appropriate number of days.

7 Select whether you want to purge, archive, or both. If you have specific purge jobs that you want to complete before a scheduled archive, ensure that you leave enough time between the purge only jobs and the archive job.

Table 25. Purge and archive options

Option	Notes
Purge events	If you select to purge events, specify the options that determine which events will be removed from the database. **All events:** Select this option to purge all events from the database that are older than the specified time. **Only selected events:** Select this option to purge only selected events, based on specific criteria, from the database that are older than the specified time. Use the criteria tabs to define the events to be deleted: - Who - purge events generated by a specific user, computer or group. - What - purge events based on subsystem, event class, object class, severity or results. - Where - purge events captured by a specific agent, domain or site. - Origin - purge events originating from a specific workstation or server. If you specify criteria on more than one tab, the criteria specified on ALL of the tabs must be met before an event is deleted from the database or archived. See Purge selected records for a description of the criteria tabs and options that appear to specify the records.
Archive events	When this option is selected, a yearly archive database will be created beginning on the first day of the selected month. For example, if you select Jan, the database will contain events for 12 months beginning on January 1.. If you have also selected to purge events based on specific criteria, any events that remain will be moved to the archive database. **NOTE:** A new archive database will be created for each year of events that you have in your production database. On initial run of archive or purge/archive job, an archive database will be created on the same database server as your production Change Auditor database. The name of the archive database is as follows: Production database name appended with _Archive_ and the year of your oldest event and a selected month. Example: ChangeAuditor_Archive_2014 _August The *.mdf file will have the same name except that the date will be appended to the end. Example: ChangeAuditor_Archive_2014__August20150310163244.mdf If the archive database is moved or deleted a new archive database with the same name will be created (the *.mdf will differ because a new date is appended) the next time an archive or purge/archive job runs. **NOTE:** If an archive database is deleted or moved before the end of an archived year, then a new one will be created and will only contain events that were not previously archived to the deleted or moved database. **NOTE:** This option is not available, if there is an existing archive job.

8 Next, set the job schedule.

Option	Description
Occurs	Specifies if the job is to be run on a weekly or monthly schedule.
	The default is monthly.
	NOTE: When **Monthly** is selected, specify the monthly schedule to be used to run the job. For example, 1 for every month (default), 2 for every other month, 6 for every six months or twice a year, etc.
Batch Limit	Specifies the maximum number of events to be purged for each cycle.
	That is, the job task checks every five minutes to determine if it needs to run a job. When the job runs, by default it purges a maximum of 500,000 events in that five minute period. If there are more than 500,000 events to be purged, then five minutes later another 500,000 events are processed until all of the events are purged or archived.If there are 500,000 events or less in a job, then the job task checks again in the next five minutes and obeys the 'next run' time.
	NOTE: If SQL is slow or disk space is low, decrease this limit to 100000 or 50000. When this limit is decreased, the job will take longer to complete.
On day of month	When a **Monthly** schedule is selected, specifies on which day of the month the job is to be run:
	• First (default)
	• Last
	• Day #
	When a **Weekly** schedule is selected, specifies the weekly schedule to be used to run the job. For example, 1 for every week, 2 for every other week, 3 for every third week, and 4 for every fourth week.
On Days	When a **Weekly** schedule is selected, defines the days of the week when the job is to be run.
	The default is Monday through Friday.
Run Time	Defines the time of day when the job is to be performed.
	The default start time is 12:00:00 AM.
	NOTE: Based on the client's current local date and time. The format used to display this date and time is determined by the local machine's regional and language setting.
Last Run	This read-only field specifies the last time (date and time) the job ran.
	NOTE: Based on the client's current local date and time. The format used to display this date and time is determined by the local machine's regional and language setting.
Next Run	This read-only field specifies the next time (date and time) when the job is scheduled to run.
	NOTE: Based on the client's current local date and time. The format used to display this date and time is determined by the local machine's regional and language setting.

9   Select **Finish**.

Purge selected records

Use the criteria tabs in the Purge and Archive wizard to define what specific records are to be deleted from the database. These tabs are enabled when you choose the **Purge | Only selected events** option.

ℹ | **NOTE:** If you specify criteria on more than one tab, the criteria specified on ALL of the tabs must be met before an event is deleted from the database or archived.

Who tab

Use the Who tab when you want to purge or archive events generated by specific users, computers, or groups. By default (when the Who tab is empty), change events generated by all users, computers, and groups will be deleted from the database or archived.

When multiple 'who' criteria is specified on this tab, Change Auditor uses the 'OR' operator to evaluate change events, purging or archiving events for activity performed by any of the users, computers or groups listed on this tab.

To purge events generated by a specific user, computer or group:

1   From the Purge and Archive wizard, select the **Purge** option, and then enable **Only selected events** to activate the criteria tabs.

2   Open the Who tab and click **Add**.

3   Use the Browse or Search page to locate the user, computer or group to be included. Once you have located a directory object, select it and click **Add** to add it to the selection list at the bottom of the dialog.

   Repeat this step to include each additional directory object.

4   After selecting one or more directory objects, click **Select** to save your selection and close the dialog.

   > **i** | **NOTE:** Use **Add with Events** (instead of **Add**) to select users, computers, or groups that already have an event associated with it in the database. Use this to purge events tied to users who have been removed from Active Directory.

5   Change Auditor will now only purge or archive events generated by the user(s), computer(s) or group(s) listed on the Who tab.

   > **i** | **NOTE:** To purge events NOT generated by the users, computers, or groups listed on the Who tab, select the **Exclude The Following Selection(s)** check box at the top of the Who tab.

To use a wildcard expression to specify users or groups:

1   From the Purge and Archive wizard, select **Purge**, and then enable **Only selected events** to activate the criteria tabs.

2   Open the Who tab and expand **Add** and click **Add Wildcard Expression**.

   > **i** | **NOTE:** If you used **Add With Events** instead, click **Add Wildcard Expression** on the Add Users, Computer, or Groups dialog.

3   On the Add Who dialog, enter the wildcard expression to be used to search for users (domain\user name) or groups (domain\group name).

   ▪   Select the comparison operator to be used: **Like** or **Not Like**

   ▪   Enter the pattern (character string and * wildcard character) to be used to search for a match. Use the * wildcard character to match any string of zero or more characters.

   ▪   By default, the wildcard expression will be used to search for users. To search for groups, select the **Group** option.

      > **i** | **NOTE:** When using the **Group** option, the Group Membership Expansion option on the Coordinator Configuration page (on the Administration Tasks tab) must be set to **Expand all groups**.

4   Click **OK** to close the dialog and add the wildcard expression to the Who tab.

5   Change Auditor will now search for and purge or archive change events generated by the users that are members of the groups whose name matches the specified wildcard expression.

What tab

Use the What tab to specify the what criteria to be used to determine whether an event is to be purged from the database. By default (when the What tab is empty), all events regardless of the subsystem, event class, object class, severity, or results will be purged or archived.

When multiple 'what' criteria is specified on this tab, Change Auditor uses the 'AND' operator to evaluate an event, purging only those events that meet all the specified criteria. However, when multiple subsystems (such as Active Directory, ADAM, and Exchange) are specified, Change Auditor uses the 'OR' operator to evaluate these entities, purging or archiving events that meet any of the specified subsystem criteria. This also applies when multiple event classes are specified. That is, when multiple event classes are specified, Change Auditor uses the 'OR' operator purging or archiving any of the specified events.

To purge events based on a specific entity:

1   From the Purge and Archive wizard, select **Purge**, and then enable **Only selected events** to activate the criteria tabs.

2   Open the What tab, expand **Add** (or **Add With Events**) and select the appropriate option. When you select an option, an additional dialog appears allowing you to enter specific criteria:

- **Subsystem | Active Directory** - Add Active Directory Container dialog
- **Subsystem | AD Query** - Add Active Directory Container dialog
- **Subsystem | ADAM (AD LDS)** - Select the agent that hosts the ADAM/LDS Instance dialog
- **Subsystem | Exchange** - Add Exchange Container dialog
- **Subsystem | Office 365 Exchange Online**- Office 365 Exchange Online dialog
- **Subsystem | File System** - Add File System Path dialog
- **Subsystem | Group Policy** - Add Group Policy Container dialog
- **Subsystem | Local Account** - Add Local Account dialog
- **Subsystem | Logon Activity** - Add Logons dialog
- **Subsystem | Registry** - Add Registry Key dialog
- **Subsystem | Service** - Add Service dialog
- **Subsystem | SharePoint** - Add SharePoint Path dialog
- **Subsystem | SQL** - Add SQL Instance dialog
- **Subsystem | VMware** - Add VMware Host dialog
- **Event Class** - Add Facilities or Event Classes dialog
- **Object Class** - Add Object Classes dialog
- **Severity** - Add Severities dialog
- **Result** - Add Results dialog

3   Once you have selected or entered the specific criteria, click **Add** to add it to the selection list at the bottom of the dialog.

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

Change Auditor will now search for and purge or archive change events that match the criteria listed on the What tab.

Where tab

Use the Where tab to purge events captured by specific agents, domains, or sites. By default (when the Where tab is empty), events captured by all agents will be purged or archived.

When multiple 'where' criteria is added to this tab, Change Auditor uses the 'OR' operator to evaluate events, purging or archiving events that were captured by any of the specified agents, domains or sites.

To purge events captured by a specific agent, domain or site:

1 From the Purge and Archive wizard, select **Purge**, and then enable **Only selected events** to activate the criteria tabs.

2 Open the Where tab and click **Add**.

3 On the Choose the Agents, Domains or Sites to Include dialog, use the Browse or Search pages to locate an individual agent, domain or site.

> **i** | **NOTE:** You can also select the Grid View option to select an agent from a list rather than using the Explorer View to locate it within your environment.

Once you have located an agent, domain or site, select it and click **Add** to add it to the selection list at the bottom of the dialog.

Repeat this step to include each additional agent, domain or site.

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

> **i** | **NOTE:** Use **Add With Events** (instead of **Add**) to select agents, domains, or sites that already have an event associated with it in the database.

5 Change Auditor will now search for and purge or archive change events captured by the agents, domains, or sites listed on the Where tab.

> **i** | **NOTE:** To purge or archive events NOT captured by the agents, domains, or sites listed on the Where tab, select the **Exclude The Following Selection(s)** check box at the top of the Where tab.

To use a wildcard expression to specify agents, domains, or sites:

1 From the Purge and Archive wizard, select **Purge**, and then enable **Only selected events** to activate the criteria tabs.

2 Open the Where tab, expand **Add** and click **Add Wildcard Expression**.

> **i** | **NOTE:** If you used **Add With Events**, click **Add Wildcard Expression** on the Add Agents, Domains, Sites dialog.

3 On the Add Where dialog, enter the wildcard expression to be used to search for agents (NetBIOS name, domains or sites.

- Select the comparison operator to be used: **Like** or **Not Like**

- Enter the pattern (character string and * wildcard character) to be used to search for a match. Use the * wildcard character to match any string of zero or more characters.

- By default, the wildcard expression will be used to search for agents. To search for domains or sites, select the **Domain** or **Site** option.

4 Click **OK** to close the dialog and add the wildcard expression to the Where tab.

Change Auditor will now search for and purge or archive change events captured by the agents, domains or sites whose name matches the specified wildcard expression.

Origin tab

Use the Origin tab to purge events originating from a specific workstation or server. By default, (when the Origin tab is empty) events will be purged regardless of the workstation or server from which they originated.

When multiple 'origin' criteria is specified on this tab, Change Auditor uses the 'OR' operator to evaluate events, purging or archiving events originating from any of the specified workstations or servers.

To purge events based on where they originated:

1 From the Purge and Archive wizard, select **Purge**, and then enable **Only selected events** to activate the criteria tabs.

2 Open the Origin tab and click **Add**.

3 On the Add Origin dialog, enter the wildcard expression to be used to include workstations or servers, based on their NetBIOS name or IP address:

  ▪ Select the comparison operator to be used: **Like** or **Not Like**

  ▪ Enter the pattern (character string and * wildcard character) to be used to search for a match. Use the * wildcard character to match any string of zero or more characters.

4 Click **OK** to close the dialog and add the wildcard expression to the Origin tab.

5 Change Auditor will now search for and purge or archive change events originating from workstations/servers whose machine name (NetBIOS name or IP address) matches the specified wildcard expression.

  ℹ | **NOTE:** To purge or archive events NOT originating from the workstations or servers listed on the Origin tab, select the **Exclude The Following Selection(s)** check box at the top of the Origin tab.

To select an originating workstation or server that has an event in the Change Auditor database:

1 From the Purge and Archive wizard, select **Purge** and then enable **Only selected events** to activate the criteria tabs.

2 Open the Origin tab and click **Add With Events**.

The Add Origin dialog appears populated with originating workstations/servers that have an event associated with it in the Change Auditor database.

  ℹ | **NOTE:** Use **Add Wildcard Expression** to enter a wildcard expression to include workstations/servers from this list based on their NetBIOS name or IP address.

3 On the Add Origin dialog, select one or more originating workstations/servers from the list and click **Add** to add it to the selection list at the bottom of the page.

4 Click **OK** to close the dialog and add the selected workstations to the Origin tab.

Change Auditor will now search for and purge or archive change events originating from the selected workstations/servers.

Report Layouts page

The Report Layouts page is displayed when **Report Layouts** is selected from the Configuration task list in the navigation pane of the Administration Tasks page. From this page you can add, edit or delete global report templates that define the header and footer information for query-based reports.

The Report Layouts page contains a list of all the report templates that have been previously defined. Initially, this list contains the Default template, which will be used for all search results reports unless changed on the Report tab of a search's Search Properties tabs.

Table 26. Report Layouts page: Tool bar buttons

Tool bar buttons	Description
Add	Use to display the New Report Layout dialog allowing you to name your new report and load the report designer to create a new report template.
Edit	Use to modify the selected report template.
Rename	Use to rename the selected report template.

Table 26. Report Layouts page: Tool bar buttons

Tool bar buttons	Description
Copy	Use to copy the selected report template. The copy will appear on the Report Layouts page.
Delete	Use to delete the selected report template.

To add a global report template:

1   Open the Administration Tasks page.

2   Click **Configuration**.

3   Select **Report Layouts** in the Configuration task list to open the Report Layouts page.

4   Click **Add** to display the New Report Layout dialog. Enter a descriptive name for the new report template and click **OK**.

The report designer appears.

5   Use the controls in the tool bar to the left of the report grid to define the header and/or footer information to be included. For example:

- To add a page header, click the **Page Header** button. Click on the report grid and the header pane will be added to the top of the page. Use the arrow controls or **Height** setting in the Properties pane to resize the header pane.

- To add the report title to the page header pane, click the **Text** button Move the pencil cursor in the heading pane where you want to place the report title and click. Open the System Variable tab in the Text Editor, locate the **ReportName** variable. Double-click the variable to add it to the text pane. Click **OK** to save your selection and close the Text Editor.

- Back on the report grid, you can resize the **ReportName** text box to prevent the report titles from being truncated. You can also use the settings in the Properties pane to modify the font, size, color, etc.

- To add a page footer (e.g., page number), click the **Page Footer** button. Click on the report grid and the page footer pane will be added to the bottom of the page. Use the arrow controls or **Height** setting in the Properties pane to resize the footer pane.

- To add the page number to the page footer pane, click the **Text** button. Move the pencil cursor in the footer pane where you want to place the page number and click. Open the System Variables tab in the Text Editor, locate the page number variable to be used (e.g., **PageNofM**). Double-click the variable to add it to the text pane. Click **OK** to save your selection and close the Text Editor.

i | **NOTE:** This is an example of how to use the report designer to add a simple header and footer. However, there are many more capabilities with the new report designer which uses StimulReport.Net components. For a detailed description and functionality of each component available for designing reports, see the Stimulsoft online help (www.stimulsoft.com).

6   After saving any changes using the Save Report button in the upper left corner of the report designer, click **Close** to return to the Report Layouts page.

The new report template is added to the Report Layouts page (Administration Tasks page) and is also now available in the **Layout** drop-down menu on the Report tab (Search Properties tabs).

Application User Interface Authorization page

The Application User Interface Authorization page is displayed when **Application User Interface** is selected from the Configuration task list in the navigation pane of the Administration Tasks page.

From this page, you can define who is authorized to perform the different operations available in the Change Auditor client, including performing the administrative tasks listed on the Administration Tasks page and defining search criteria.

Table 27. Application User Interface Authorization page: Tool bar buttons

Tool bar buttons	Description
Add | Add Role Definition	Use to define a new role defining who is authorized to perform the selected tasks and/or operations.
Add | Add Task Definition	Use to define a new task defining the operations that can be performed.
Add | Add Application Group	Use to define a new Authorization Manager Application Group.
Edit	Use to edit the selected item. **NOTE:** The Administrator, Operator, and Web Client Shared Overview roles and tasks cannot be edited.
Delete	Use to delete the selected item. **NOTE:** The Administrator, Operator, and Web Client Shared Overview roles and tasks cannot be deleted.

To add a task definition:

A task is a collection of operations and sometimes lower-level tasks that can be performed.

1 Open the Administration Tasks page.

2 Click **Configuration**.

3 Select **Application User Interface** in the Configuration task list to open the Application User Interface Authorization page.

4 Expand **Add** and click **Add Task Definition**.

5 Enter the following information on the Authorizations: Task dialog:

Table 28. Authorizations: Task dialog

Tab	Description	Procedure	
Task	Name the task	1	Enter a name for the task.
		2	Enter a brief description of the task.
Definition	Add the operations and lower-level tasks that can be performed	•	To add a lower-level task, click **Add Task** and select a task from the Authorizations: Task Definitions dialog.
		•	To add an operation, click **Add Operation** and select one or more operations from the Authorizations: Operations dialog.

6 Click **OK** to save your new task definition and close the Authorizations: Task dialog.

This task will now be included in the task list on the Authorizations: Task Definitions dialog and can be included in a role definition.

Task definitions are also listed on the Application User Interface Authorization page.

To add a role definition:

A role definition defines who is authorized to perform specific tasks and/or individual operations in the client. A role usually corresponds to a job function or responsibility and consists of a collection of tasks that a user must be authorized to perform to do their job function.

1 Open the Application User Interface Authorization page.

2 Click **Add** and click **Add Role Definition**.

3   Enter the following information on the Authorizations: Role dialog:

Table 29. Authorizations: Role dialog

Tab	Description	Procedure	
Role	Name the role	1	Enter a name for the role.
		2	Enter a brief description of the role.
Definition	Add a role, task or operation to the role	•	To add a role, click **Add Role** and select a role from the Authorizations: Role Definitions dialog.
		•	To add a task, click **Add Task** and select a task from the Authorizations: Task Definitions dialog.
		•	To add an operation, click **Add Operation** and select one or more operations from the Authorizations: Operations dialog.
Members	Add a user, group or application group to the role	•	To add an application group, click **Add Application Group** and select an application group from the Authorizations: Application Groups dialog.
		•	To add a user or group, click **Add User or Group**, which displays the Select Users and Groups dialog. Use the Browse page or Search page to locate and select the user and/or group accounts to be added
		NOTE: f a user or group account is added to multiple access roles, the account will have the authority to perform the operations defined in the more authoritative role.	

4   Click **OK** to save your new role definition and close the Authorizations: Role dialog.

Role definitions are displayed on the Application User Interface Authorization page.

To add an application group:

Application groups allow you an alternate way of assigning users to roles. An application group is a feature of Windows Authorization Manager (AzMan) where you can define a group of users without having to go through your domain administrator to add a new group to Active Directory.

1   Open the Application User Interface Authorization page.

2   Expand **Add** and click **Add Application Group**.

3   Enter the following information on the On the Group tab of the Authorizations: Group dialog, enter the following information:

Table 30. Authorizations: Group dialog

Tab	Description	Procedure
Group	Name the application group	1 Enter a name for the application group. 2 Enter a brief description for the application group. 3 Select one of the following methods which is to be used to define a group of users: ▪ Basic (default) ▪ LDAP Query **NOTE:** Basic groups are a lot like Active Directory groups; however you can define both included and excluded members. LDAP query groups allow you to define an LDAP query to dynamically create a group of users who are similar. Refer to the Windows Authorization Manager documentation for more information on basic and LDAP query groups.
Members	Add the users and groups that are to be members of the application group	• To add an application group, click **Add Application Group** and select an application group from the Authorizations: Application Groups dialog. • To add a user or group, click **Add User or Group**, which will display the Select Users and Groups dialog. Use the Browse page or Search page to locate and select the users and/or groups to be added.
NonMembers	Add users and groups to be excluded from the application group	• To add an application group, click **Add Application Group** and select an application group from the Authorizations: Application Groups dialog. • To add a user or group, click **Add User or Group**, which will display the Select Users and Groups dialog. Use the Browse page or Search page to locate and select the users and/or groups to be added.

4   Click **OK** to save your new application group and close the Authorizations: Group dialog.

When the selected members now try to define Active Directory protection they will be restricted to defining protection for the selected domain or organizational unit.

Auditing Tasks (Administration Tasks Page)

- Introduction
- Configuration
- Forest
- Applications
- Server
- NAS

Introduction

The following sections describe the pages and tasks available through the Auditing task list of the Administration Task page. The auditing pages allow you to enable and disable events, define custom auditing definitions for your Active Directory forest, define auditing for different types of applications within your environment, create auditing templates that can then be assigned to agent configurations to enable custom server-level auditing, and create auditing templates for NAS devices. For a full description of all the options and fields available on the Auditing tasks pages, refer to the appropriate Change Auditor user guide.

The Auditing task list is divided into the following separate task lists:

- Configuration
  - Audit Events
  - Excluded Accounts auditing
- Forest
  - Active Directory auditing
    - AD Attribute Auditing page
    - Member of Group Auditing page
    - AD Query Auditing page
  - ADAM (AD LDS) auditing
    - ADAM (AD LDS) Attribute Auditing page
- Applications
  - Exchange Mailbox auditing
  - Office 365 and Azure Active Directory auditing
  - SQL auditing
  - VMware auditing
  - SharePoint auditing

- Server
  - File System auditing
  - Registry auditing
  - Services auditing
- NAS
  - EMC auditing
  - NetApp auditing
  - Fluid File System (FluidFS) auditing

i | **NOTE:** Authorization to use the administration tasks on the Administration Tasks page is defined using the Application User Interface page. If you are denied access to the tasks on any of these pages, refer to Application User Interface Authorization page.

Configuration

The tasks under this heading are used for configuring the events to captured and the accounts to exclude from auditing.

See the following administration task descriptions for more information:

- Audit Events
- Excluded Accounts auditing

Audit Events

You can enable and disable the auditing of individual events so that Change Auditor audits only those events that are vital to your organization's operation. In addition, you can modify the severity level (high, medium, or low) and description assigned to each event. Change Auditor uses the severity level when processing events to help you in determining the potential level of risk associated with each configuration change event.

Audit Events page

The Audit Events page is displayed when **Audit Events** is selected from the Auditing task list in the navigation pane of the Administration Tasks page, and it lists all the events available for auditing by Change Auditor. It displays the facility to which the event belongs, the event severity, if the event is enabled or disabled and the required Change Auditor license.

i | **NOTE:** Changes made on this page are global and apply to all agents.

i | **NOTE:** For more information, including a full description of the page, refer to the Change Auditor User Guide.

Table 31. Audit Events page: Tool bar buttons

Tool bar buttons	Description
Columns	Use to display different fields on the Audit Events page.
Edit	Use to edit the description of the selected event.
High | Medium | Low	Use to change the severity of the selected event.
Enable	Use to enable the selected event.

Table 31. Audit Events page: Tool bar buttons

Tool bar buttons	Description
Disable	Use to disable the selected event.
Default	Use to reset the selected event's severity, description, and enable or disable status back to the factory defaults.
Knowledge Base	Use to launch the knowledge base entry for the selected event.

Right-click commands are also available when you right-click an event in the grid. In addition to the event-related actions, you can also change the results criteria for capturing an event.

To change the results criteria for capturing an event:

1   Open the Audit Events page.

2   Right-click the event to modify and select one of the following options:

- All Results (default)

- Success Only

- Success and Protected Only

- Success and Failed Only

Change Auditor will now only capture and return the event if the operation mentioned in the event meets the results criteria selected.

Excluded Accounts auditing

Account exclusion allows you to define a list of trusted accounts to exclude are from auditing. This enables you to exclude events generated by accounts that make many changes or by accounts which are trusted.

To use the account exclusion feature, you must first complete the following steps to define the user and computer accounts that can make changes without triggering an event in Change Auditor:

1   Create an Excluded Accounts template which specifies the user and/or computer accounts to exclude from auditing.

2   Add this template to an agent configuration. (See Define agent configurations.)

3   Assign the agent configuration to Change Auditor agents. (See Assign agent configurations to agents.)

Excluded Accounts Auditing page

The Excluded Accounts Auditing page is displayed when **Excluded Accounts** is selected from the Auditing task list in the navigation pane of the Administration Tasks page. It contains an expandable view of all the Excluded Accounts templates that have been defined. From this page, you can launch the Excluded Accounts wizard to create a template. You can also edit existing templates, disable and enable templates, or remove templates that are no longer being used.

ℹ️ | **NOTE:** For more information, including a full description of the page, refer to the Change Auditor User Guide.

To create an Excluded Accounts template:

1   Open the Administration Tasks page.

2   Click **Auditing**.

3   Select **Excluded Accounts** (under the Configuration heading in the Auditing task list) to open the Excluded Accounts Auditing page.

4   Click **Add** to open the Excluded Accounts wizard which steps you through the process of creating an Excluded Accounts template.

Table 32. Excluded Accounts Wizard

Page	Description	Procedure
Welcome	Name your template.	1 Enter a name for the template. 2 Click **Next**.
Account Selection	Select the accounts to exclude. See Directory object picker for a detailed description of this wizard page.	1 From the Browse or Search page, select an account and click **Add** to add it to the selection list. 2 (Optional) To specify a wildcard search expression to dynamically exclude additional user accounts from auditing, use the **(Optional) Enter an account name wildcard** field. In the text box, enter the wildcard expression (string of characters and/or wildcard character) to be used to search the Domain (NetBIOS)\NT 4 account name for matching users: ▪ Use an asterisk (*) to substitute zero or more alphanumeric characters. ▪ Use a question mark (?) to substitute a single alphanumeric character. Click **Add Wildcard** to add it to the selection list. 3 Click **Next**.
Event/Facility Selection	Select the event classes and facilities to exclude.	1 Select the event classes and facilities to exclude. 2 Select one of the following options to add it to the selection list: ▪ **Add**	**Add This Event** to add individual events. ▪ **Add**	**Add All Events In Facility** to add all events in the selected facility. 3 Click **Finish** to save the template and close the wizard.

Forest

The tasks under this heading are used to define custom auditing definitions for your Active Directory forest.

See the following administration task descriptions for more information:

- Active Directory auditing
- ADAM (AD LDS) auditing
- Applications

Active Directory auditing

By default, Change Auditor for Active Directory audits the Enterprise for changes made to the user, group, and computer objects. However, using the Active Directory auditing tasks you can specify where to conduct the audit (Enterprise, an individual object, and so on) and what to audit, such as the object classes, individual attributes, and even users based on group membership.

In addition, if you have Change Auditor for Active Directory Queries licensed, you can specify Active Directory containers to exclude from AD query auditing.

See the following Administration Tasks page descriptions for more information:

- Active Directory Auditing page
- AD Attribute Auditing page
- Member of Group Auditing page
- AD Query Auditing page

Active Directory Auditing page

The Active Directory Auditing page opens when **Active Directory** is selected from the Auditing task list in the navigation pane of the Administration Tasks page, and contains an expandable view of the Active Directory objects selected for auditing. Initially, the list box contains an entry for auditing all user, computer, and group object classes in the entire enterprise.

> **i** | **NOTE:** For more information, including a full description of the page, refer to the Quest Change Auditor for Active Directory User Guide.

To add an Active Directory object to the auditing list:

1 Open the Administration Tasks page.

2 Click **Auditing**.

3 Select **Active Directory** in the Auditing task list to display the Active Directory Auditing page.

4 Click **Add** to open the Active Directory Auditing wizard, which steps you through the process of defining the objects and object classes to audit.

Table 33. Active Directory Auditing Wizard

Page	Description	Procedure

Object Selection	Select the Active Directory objects to audit.
	
	See Directory object picker for a detailed description of this wizard page.
		1 Select where to conduct the audit:
		
		  ▪ Enterprise
		
		  ▪ This Object
		
		  ▪ This Object and Child Object Only
		
		  ▪ This Object and All Child Objects
		
		2 If you selected the **This Object**, **This Object and Child Objects Only** or **This Object and All Child Objects** option, use the Browse or Search pages to locate the directory object or container to be audited.
		
		If required, use the Forest drop-down box to select in which forest the objects reside. Foreign agent forests may require foreign forests credentials which can be entered on the Credentials Required dialog.
		
		3 Click **Next**.

Object Classes	Select object classes to audit under the selected container. **NOTE:** At least 1 object class must be selected for auditing.	1 Select one or more object classes in the Unaudited Object Class list (left pane) 2 Click **Add** to move it to the Audited Object Class list (right pane). 3 Click **Finish** to save your selection and close the wizard.

AD Attribute Auditing page

The AD Attribute Auditing page is displayed when **Active Directory | Attributes** is selected from the Auditing task list in the navigation pane of the Administration Tasks page. Using the AD Attribute Auditing feature, you can customize Change Auditor to meet your auditing requirements by specifying the individual schema attributes to be audited. In addition to specifying individual attributes for auditing, you can also assign a severity.

i | **NOTE:** For more information, including a full description of the page, refer to the Quest Change Auditor for Active Directory User Guide.

To define custom attribute auditing:

1 Open the Administration Tasks page.

2 Click **Auditing**.

3 Select **Attributes** under Active Directory in the Auditing task list to open the AD Attribute Auditing page.

4 Select an object class from the list and click **Edit**.

The Active Directory Attributes Auditing Wizard dialog appears, which contains a list of the attributes available for the selected object class.

5 In the Unaudited Attribute list (left pane) select one or more attributes and click **Add** to select them for auditing.

6 To change the severity level assigned to an attribute, in the right pane, click in the **Severity** cell and use the drop-down arrow to select the severity you want to assign to the selected attribute.

7 To remove an attribute from auditing, select the attribute from the right pane and click **Remove**. Selecting this button moves the selected attribute back into the Unmonitored Attribute list.

8 Click **Finish** to save the selected attributes and close the dialog.

9   Once you have selected at least one attribute for auditing, the associated Audited Attributes column will display the number of attributes selected for auditing. This value will also be displayed in the **Audited Attributes** column back on the Active Directory Auditing page.

Member of Group Auditing page

The Member of Group Auditing page is displayed when **Member of Group** is selected from the Auditing task list in the navigation pane of the Administration Tasks page. Using the Member of Group Auditing feature, you can customize Change Auditor to meet your auditing requirements by specifying the users to be audited based on their group membership.

> **i** | **NOTE:** For more information, including a full description of the page, refer to the Quest Change Auditor for Active Directory User Guide.

To add a group to the Member of Group Auditing list:

1   Open the Administration Tasks page.

2   Click **Auditing**.

3   Select **Active Directory** under the Auditing task list to display the Active Directory Auditing page. Check to ensure that the user object class is removed from auditing and NOT listed on this page. If it is still listed, select it and click **Delete | Delete Object Class** to remove it from the Active Directory auditing list.

4   Once the user object class has been removed, select **Member of Group** in the Auditing task list to display the Member of Group Auditing page.

5   Click **Add** to display the Member of Group Auditing wizard to locate and select the groups whose users are to be audited by Change Auditor.

6   Use the Browse and Search pages to locate and select a group and click **Add** to add the selected group to the selection list.

     Repeat this step to add additional groups to the Member of Groups Auditing list.

7   Click **Finish** to save your selections, close the wizard and return to the Member of Group Auditing page, where your selections will now be listed.

AD Query Auditing page

The AD Query Auditing page displays when you select **AD Query** from the Auditing task list in the navigation pane of the Administration Tasks tab. From this page you can specify the Active Directory containers to include and exclude in Active Directory query auditing.

> **i** | **NOTE:** By default, all containers are included

> **i** | **NOTE:** Due to the high volume of Active Directory queries performed against the Schema, RootDSE, and the Configurations containers, Quest recommends that you add these to the exclusion list.

Inclusion and exclusion rules

Only objects that are included (and not excluded) are monitored. For example:

- When an object is included and excluded at the same time, it will not be monitored.

- When an object is included and some of its child objects are excluded, only child objects that are not excluded will be monitored.

- When an object is excluded and some of its child objects are included, none of the child objects will be monitored.

> **i** | **NOTE:** For more information, including a full description of the page, refer to the Change Auditor for Active Directory Queries User Guide.

To include a container to the AD Query audit list:

1   Open the Administration Tasks tab.

2   Click **Auditing**.

3   Select **AD Query** (under the Forest heading in the Auditing task list) to open the AD Query Auditing page.

4   Click **Add** to open the AD Query Auditing wizard.

5   Select one of the scope options at the top of the page:

  ▪ **RootDSE** - select this option to include the RootDSE object.

  ▪ **This Object and All Child Objects** - select this option to specify the containers to include. (Selecting a container will also include any child objects.)

6   If the **This Object and All Child Objects** option is selected, use the Browse and Search pages to locate and select a directory object. Click **Add** to add the selected directory object to the list at the bottom of the page.

    Repeat this step to add additional directory objects.

7   Click **Finish** to close the wizard and return to the AD Query Auditing page, where your selections will now be listed.

To exclude a container to the AD Query audit list:

1   Open the Administration Tasks tab.

2   Click **Auditing**.

3   Select **AD Query** (under the Forest heading in the Auditing task list) to open the AD Query Auditing page.

4   Click **Add** to open the AD Query Auditing wizard.

5   Select one of the scope options at the top of the page:

  ▪ **RootDSE** - select this option to exclude the RootDSE object. (Selecting this container will not exclude child objects.)

  ▪ **This Object and All Child Objects** - select this option to specify the containers to exclude. (Selecting a container will also exclude any child objects.)

6   If the **This Object and All Child Objects** option is selected, use the Browse and Search pages to locate and select a directory object. Click **Add** to add the selected directory object to the list at the bottom of the page.

    Repeat this step to add additional directory objects.

7   Click **Finish** to close the wizard and return to the AD Query Auditing page, where your selections will now be listed.

ADAM (AD LDS) auditing

Change Auditor for Active Directory allows you to audit Active Directory Application Mode (ADAM) and Active Directory Lightweight Directory Services (AD LDS) events. Use the ADAM (AD LDS) Auditing tasks to define the ADAM instances, the directory objects or containers, the object classes and optionally the individual attributes to be audited.

See the following Administration Tasks page descriptions for more information:

•   ADAM (AD LDS) Auditing page

•   ADAM (AD LDS) Attribute Auditing page

ADAM (AD LDS) Auditing page

The ADAM (AD LDS) Auditing page is displayed when **ADAM (AD LDS)** is selected from the Auditing task list in the navigation pane of the Administration Tasks page. Use the ADAM (AD LDS) Auditing page to create a list of ADAM instances, directory objects or containers, and object classes to be audited.

i | **NOTE:** For more information, including a full description of the page, refer to the Change Auditor for Active Directory User Guide.

To enable ADAM (AD LDS) auditing:

1   Open the Administration Tasks page.

2   Click **Auditing**.

3   Select **ADAM (AD LDS)** in the Auditing task list to open the ADAM (AD LDS) Auditing page.

4   Click **Add** to launch the ADAM (AD LDS) Auditing wizard.

Table 34. ADAM (AD LDS) Auditing Wizard

Page	Description	Procedure
ADAM (AD LDS) Instance	Select the ADAM (AD LDS) instance from which to choose audited objects and enter the credentials for a user with access to the instance.	1 Select an ADAM (AD LDS) instance from the list. 2 Enter the Domain\User Name and Password of a user who can access the selected ADAM (AD LDS) instance. 3 Click **Test** to verify the credentials. 4 Click **Next**. **NOTE:** If you have multiple ADAM (AD LDS) instances with replicating application partitions, there is no need to configure an auditing template for each instance. Change Auditor will automatically send the auditing configuration to each machine that is hosting an instance. You must have an agent installed on each instance host.
Object Selection	Select where to conduct the audit. See Directory object picker for a detailed description of this wizard page.	1 Select where to conduct the audit. 2 From the Browse or Search page, select the ADAM (AD LDS) object or container to be audited. 3 Click **Next**.
Object Classes	Select object classes to audit under the selected container. **NOTE:** At least one object class must be selected for auditing.	1 Select one or more object classes in the Unaudited Object Class list (left pane) 2 Click **Add** to move it to the Audited Object Class list (right pane). 3 Click **Finish** to save your selections and close the wizard.

ADAM (AD LDS) Attribute Auditing page

The ADAM (AD LDS) Attribute Auditing page is displayed when **ADAM (AD LDS) | Attributes** is selected from the Auditing task list in the navigation pane of the Administration Tasks page. Using the ADAM (AD LDS) Attribute

Auditing feature, you can specify the individual schema attributes to be audited for the selected object class(es). In addition to specifying individual attributes for auditing, you can also assign a severity.

> **i** | **NOTE:** For more information, including a full description of the page, refer to the Change Auditor for Active Directory User Guide.

To audit attributes for selected object classes:

1 Open the Administration Tasks page.

2 Click **Auditing**.

3 Select **Attributes** under ADAM (AD LDS) in the Auditing task list to open the AD Attribute Auditing page.

4 Select an object class from the list and click **Edit**.

The ADAM (AD LDS) Attributes Auditing wizard appears, which contains a list of the attributes available for the selected object class.

5 In the Unaudited Attribute list (left pane), select one or more attributes and click **Add** to select them for auditing.

6 To change the severity level assigned to an attribute, in the right pane, click in the **Severity** cell and use the drop-down arrow to select the severity you want to assign to the selected attribute.

7 To remove an attribute from auditing, select the attribute from the right pane and click **Remove**. Selecting this button moves the selected attribute back into the Unaudited Attribute list.

8 Click **Finish** to save the selected attributes, close the dialog and return to the ADAM (AD LDS) Attribute Auditing page.

Once you have selected at least one attribute for auditing, the associated Audited Attributes column will display the number of attributes selected for auditing. This value will also be displayed in the Audited Attributes column back on the ADAM (AD LDS) Auditing page.

Applications

The tasks under this heading are used to define auditing for different types of applications within your environment.

See the following administration task descriptions for more information:

- Exchange Mailbox auditing
- Office 365 and Azure Active Directory auditing
- SQL auditing
- VMware auditing
- SharePoint auditing

Exchange Mailbox auditing

Exchange Mailbox auditing helps tighten enterprise-wide change and control policies by tracking user and administrator activity such as user account changes, delivery restriction changes, send on behalf updates, and more. With these types of real-time alerts and in-depth analysis and reporting capabilities, your Exchange infrastructure is always protected from exposure to suspicious behavior or unauthorized access and kept in compliance with corporate and government standards.

> **i** | **NOTE:** For more information, including important tips and a full description of the following page, refer to the Quest Change Auditor for Exchange User Guide.

To enable Exchange Mailbox auditing, you must first define whose (users or groups) mailbox activities are to be audited.

1   Define an Exchange Mailbox Auditing list that contains the directory objects whose mailbox activities you want to audit.

2   In Change Auditor, some of the Exchange Mailbox events are disabled by default due to the potentially high volume of events that can occur. If you want to capture audit events for any of these disabled events, you will need to enable them.

> **i** | **IMPORTANT:** When the **Message read by non-owner** event is enabled and a mailbox is moved from one mailbox store to another, Change Auditor generates an event for every email in the mailbox that is being moved. For example, if a user has 1,000 emails in his/her mailbox, you will receive 1,000 Message read by non-owner events in Change Auditor.
>
> To avoid generating these events, do not add the user account for the mailbox to be moved to the list on the Exchange Mailbox Auditing page on the Administration Tasks page.

Exchange Mailbox Auditing page

To enable Exchange mailbox auditing, you must first specify whose mailbox activities are to be audited. To create this mailbox list, use the Exchange Mailbox Auditing page, which is displayed when **Exchange Mailbox** is selected from the Auditing task list in the navigation pane of the Administration Tasks page.

> **i** | **NOTE:** The directory objects listed on this page only apply to the events contained in the Exchange Mailbox Monitoring and Exchange ActiveSync Monitoring facilities. This list does not apply to any of the other Exchange facilities.

To include an Exchange Mailbox in the auditing process:

1   Open the Administration Tasks page.

2   Click **Auditing**.

3   Select **Exchange Mailbox** (under the Applications heading in the Auditing task list) to open the Exchange Mailbox Auditing page.

4   Click **Add** to display the Exchange Auditing wizard.

5   Select one of the options at the top of the page: **Enterprise** or **This Object** (default).

6   If the **This Object** option is selected, use the Browse and Search pages to locate and select a directory object (i.e., User, Group, Container, DomainDNS, OrganizationalUnit, or BuiltinDomain) and use **Add** to add the selected directory object to the selection list at the bottom of the page.

    Repeat this step to add additional directory objects to the Exchange Mailbox Auditing list.

7   Click **Finish** to close this wizard and return to the Exchange Mailbox Auditing page, where your selections will now be listed with a **No** in the **Exclude** cell.

8   By default, only Non-Owner events are selected for auditing.

    For individual user mailboxes, you can change this to include 'By Owner' events as well. To do this, click in the **Events** cell and select the **Owner, Non-Owner** option from the list.

> **i** | **NOTE:** Selecting 'By Owner' auditing for many mailboxes can produce very large numbers of events. This adversely affects Change Auditor auditing and in severe cases the performance of the Exchange Server itself. In extreme cases, Outlook connections may be slowed or dropped. Select owner auditing for at most only a small number of critical mailboxes.

> **i** | **NOTE:** 'By Owner' events are disabled by default. You will need to enable these events from the Audit Events page on the Administration Tasks page before Change Auditor will capture these events.

> **i** | **NOTE:** Auditing normal mailboxes where access permission is granted to many delegates (more than 10), can produce large numbers of non-owner events. This will adversely affect Change Auditor auditing and in severe cases, the performance of the Exchange Server itself. If these mailboxes need to be audited, add them to the Shared Mailbox list (User Defined tab) to reduce unwanted non-owner events and to improve performance. See the Quest Change Auditor for Exchange User Guide for more information.

9   The default scope of coverage is displayed in the **Scope** cell. You can change this by clicking in the **Scope** cell and selecting the appropriate option from the list:

- **Object** - to audit an individual object

- **One Level** - to audit an object and its direct child objects

- **Subtree** - to audit an object and all of its subordinate objects (all levels)

To exclude an Exchange Mailbox in the auditing process:

From the Exchange Mailbox Auditing page you can exclude a previously included mailbox by changing the setting in the **Exclude** cell.

1   From the Exchange Mailbox Auditing page you can exclude a previously included mailbox by changing the setting in the **Exclude** cell. Use one of the following methods:

- Click in the **Exclude** cell of the mailbox to be included and select **Yes.**

- Right-click the mailbox entry and click **Exclude**.

2   The Exchange mailbox is now excluded from auditing.

For example, if you wanted to audit all mailboxes in the Enterprise, except those belonging to the accounts in the ExchangeAdmin organizational unit, you would create two entries in the Exchange Mailbox Auditing list:

- Use **Add** to create an audit entry for the **Enterprise** with **Exclude = No**.

- Use **Add** to create an audit entry for the **ExchangeAdmin OU** and change **Exclude** to **Yes**.

Office 365 and Azure Active Directory auditing

Change Auditor provides extensive, customizable auditing of critical activities and provides detail alerts about vital changes taking place in Microsoft Office 365 Exchange Online, SharePoint Online, OneDrive for Business, and Azure Active Directory. Continually being in-the-know helps you to prove compliance, drive security, and improve uptime while proactively auditing changes to configurations and permissions.

To ensure Office 365 and Azure Active Directory compliance, you can generate intelligent, in-depth reports, protecting you against policy violations and avoiding the risks and errors associated with day-to-day modifications. By correlating activity across the on-premises and cloud environment, you can easily search all events regardless of where they occurred

To audit Office 365 Exchange Online, SharePoint Online, OneDrive for Business and Azure Active Directory you must first create an auditing template that defines the service and for Exchange Online the type of events (mailbox and administration cmdlet) to audit and the Change Auditor agent to assign. This can only be configured through the Windows client. For more information, see the Office 365 and Azure Active Directory Auditing User Guide.

SQL auditing

To enable SQL Server auditing, you must add a SQL Auditing template to an agent configuration, which can then be assigned to the appropriate agents. Change Auditor ships with a pre-defined SQL Auditing template that can be used to audit key events on the default SQL server instance or you can create a new SQL auditing template to specify the SQL instances and SQL Server operations to be audited.

🛈 **IMPORTANT:** When multiple SQL Auditing templates are assigned to an agent configuration, the criteria specified in the last template assigned to the agent takes precedence.

SQL Auditing page

The SQL Auditing page is displayed when **SQL** is selected from the Auditing task list in the navigation pane of the Administration Tasks page, and contains an expandable view of all the SQL Auditing templates that have been defined. From this page you can launch the SQL Auditing wizard to specify the SQL instances and the operations

to be audited. You can also edit existing templates, copy templates, disable/enable templates, or remove templates that are no longer being used.

> **i** | **NOTE:** For more information, including important tips and a full description of the following page, refer to the Quest Change Auditor for SQL Server User Guide.

To create a new SQL auditing template:

1   Open the Administration Tasks page.

2   Click **Auditing**.

3   Select **SQL** (under the Applications heading in the Auditing task list) to open the SQL Auditing page.

4   Click **Add** to open the SQL Auditing wizard which steps you through the process of creating a SQL Auditing template.

Table 35. SQL Auditing Wizard

Page	Description	Procedure
Welcome	Name your template.	1 Enter a name for the template. 2 Click **Next**.
SQL Instances	Select the SQL instance(s) to be audited.	1 Click **Add** to open a drop-down list and select the SQL instance to add: ▪ **Default** ▪ **Named** (enter the name of the SQL instance) ▪ **All Instances** 2 Click **Next**.
SQL Events	Select the operations (facilities or event classes) that are to be audited. **NOTE:** At least one event must be selected.	1 Select an operation to be audited 2 Select one of the following options to add it to the selection list: ▪ **Add | Add This Event** to add individual events. ▪ **Add | Add All Events in Facility** to add all events in the selected facility. 3 Click **Next**. **NOTE:** Clicking **Finish** saves the template and closes the wizard.

Table 35. SQL Auditing Wizard

Page	Description	Procedure
SQL Column Filters	(Optional) Define column filters to capture only a subset of transactions.	1 Select a filter. 2 Click **Add** to add it to the selection list. 3 From the selection list, click in the **Operator** cell to change the operator. 4 Click in the **Value** cell to enter the value or string to be used in the filtering. **NOTE:** When multiple filters are specified these filters are 'ANDed' together and all filters must be met in order to be considered a match. To use the 'OR' operator instead, click in the left-most column of a column filter row and select OR from the drop-down. When filters are 'ORed' together, then only one of the filters must be met in order to be considered a match. **NOTE:** When both 'AND' and 'OR' operators are present in the filter list, 'ORed' filters are evaluated first and their results are used by the 'AND' filter. 5 Click **Finish** to save the template and close the wizard.

VMware auditing

To enable VMWare auditing, you must first create a VMware Auditing template which specified the VMware hosts to be audited and the agent to be used to monitor the selected VMware hosts.

> **NOTE:** If you add multiple machines (for example, vCenter Servers and/or ESX hosts) to a single auditing template, all of these computers must use the same credentials. If you want to audit machines that use different credentials, you must create a different VMware Auditing template for each of these machines.

VMware Auditing page

The VMware Auditing page is displayed when **VMware** is selected from the Auditing task list in the navigation pane of the Administration Tasks page. This page contains an expandable view of all the VMware Auditing templates that have been previously defined. From this page you can launch the VMware Auditing wizard to define VMware Auditing templates specifying the VMware hosts to be audited.

> **NOTE:** For more information, including a full description of the page, refer to the Change Auditor User Guide.

To create a VMware auditing template:

1. Open the Administration Tasks page.

2. Click **Auditing**.

3. Select **VMware** (under the Applications heading in the Auditing task list) to open the VMware Auditing page.

4. Use **Add** to launch the VMware Auditing wizard which steps you through the process of creating a VMware Auditing template.

Table 36. VMware Auditing Wizard

Page	Description	Procedure
Welcome	Name your template.	1 Enter a name for the template. 2 Click **Next**.

Table 36. VMware Auditing Wizard

Page	Description	Procedure
VMware Hosts	Select the VMware hosts to be audited.	1 Click **Add** to create a blank line in which to enter the IP address or name (the name entered must be resolvable) of the vCenter Server or of an individual host computer to audit. 2 To edit the port number, click in the **Port** cell to the right of the host name and use the arrow controls. 3 To audit one or more hosts on a specific vCenter Server, expand **Add** and click **Find ESX Hosts**. The Find ESX Hosts dialog appears: ▪ Enter the IP address or name (and port) of the vCenter Server to find ESX hosts for. ▪ Enter the user name and password of an account with access. ▪ Click **Find ESX Hosts.** ▪ Select one or more hosts. ▪ Click **OK** to close the dialog. 4 Click **Next**.
Agent Selection	Select the agent to be used to monitor the selected VMware hosts and enter the credentials to be used to access the VMware hosts. NOTE: The agent must have access to the vCenter Server or VMware host(s) selected on the previous wizard page and all of those machines must use the same credentials IMPORTANT: You can select an account with 'Read-Only' access or role (for restrictions) to properly audit VMware events. The credentials entered may be Active Directory or Linux® credentials depending on the machine (vCenter Server vs. individual host computer) selected for auditing.	1 Click **Browse** to open the VMware dialog. 2 Select an agent from the list, enter the credentials and then click **OK** to close the dialog. 3 A certificate notice is displayed for each machine selected for auditing. Click **OK** to accept the certificates. 4 Click **Finish** to save the template and close the wizard.

SharePoint auditing

To enable SharePoint auditing, you must deploy the Change Auditor SharePoint component to the SharePoint farms to be audited by Change Auditor, then create a SharePoint Auditing template for each SharePoint farm to be audited. The SharePoint Auditing template also defines the paths within the farm that are to be audited and specifies the agent to be used to capture the SharePoint events for the selected SharePoint farm.

SharePoint Auditing page

The SharePoint Auditing page is displayed when **SharePoint** is selected from the Auditing task list in the navigation pane of the Administration Tasks page, and contains an expandable view of all the SharePoint Auditing templates that have been defined. From this page you can launch the SharePoint Auditing wizard to specify the SharePoint farm and paths to be audited. You can also edit existing templates and remove templates that are no longer being used.

> **i** | **NOTE:** For more information, including a full description of the page, refer to the Quest Change Auditor for SharePoint User Guide.

To create a new SharePoint Auditing template:

1 Open the Administration Tasks page.

2 Click **Auditing**.

3 Select **SharePoint** (under the Applications heading in the Auditing task list) to open the SharePoint Auditing page.

4 Use **Add** to launch the SharePoint Auditing wizard which steps you through the process of creating a SharePoint Auditing template.

Table 37. SharePoint Auditing Wizard

Page	Description	Procedure
SharePoint Farm	Select the SharePoint farm to audit.	1 Click **Find a SharePoint farm** to select a SharePoint farm for auditing.
		2 Select from a list of agents that host a SharePoint farm and enter credentials to access the farm. Click **OK** to close the dialog.
		3 Click **Next**.
SharePoint Paths	Select the SharePoint paths to be audited and excluded from auditing.	1 Click **Add** at the top of the page to open the Browse SharePoint dialog.
		2 On this dialog, locate and select the paths to be audited. Click **OK** to close the dialog and add the path(s) to the SharePoint paths to audit list (top pane).
		3 (Optional) On the **Add optional SharePoint paths to exclude from auditing under** pane, select a path that has been added to the SharePoint paths to audit list (top pane) and then click the **Add** button to locate and add any subsequent paths within the selected path that are to be excluded from auditing. Click **OK**.
		4 Click **Next**.

Table 37. SharePoint Auditing Wizard

Page	Description	Procedure
SharePoint Events	Select the operations (facilities or event classes) to be audited. **NOTE:** At least one event must be selected.	1 Select the event classes and/or facilities to exclude. 2 Select one of the following to add it to the selection list: ▪ **Add** | **Add This Event** to add an individual event. ▪ **Add** | **Add All Events In Facility** to add all events in the selected facility. 3 Click **Next**.
Agent Selection	Select the agent to be used to monitor the specified SharePoint farm.	1 Click **Browse** to display the SharePoint farm dialog. 2 Select an agent from the list, enter the credentials and then click **OK**. 3 Click **Next**.
Solution Status	Verify that the Change Auditor SharePoint Solution has been added and deployed to each SharePoint farm selected for auditing.	1 Verify that the solution has been added and deployed. 2 (Optional) Click the **Refresh Change Auditor Solution Status** button to force a refresh of the solution's status. 3 Click **Finish** to save the template and close the wizard.

Server

The tasks under this heading are used to create auditing templates that, once assigned to agent configurations, enable custom server-level auditing. After creating a template, see Agent Configuration page for information on enabling these templates.

See the following administration task descriptions for more information:

- File System auditing
- Registry auditing
- Services auditing

File System auditing

To capture Windows File Server events, you must first complete the following steps to define the files/folders to be audited and the events to be captured:

1 Create a File System Auditing template which specified the files/folders and events to be audited.

2 Add this template to an agent configuration. (See Define agent configurations.)

3 Assign the agent configuration to agents. (See Assign agent configurations to agents.)

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

File System Auditing page

The File System Auditing page is displayed when **File System** is selected from the Auditing task list in the navigation pane of the Administration Tasks page. From this page you can launch the File System Auditing wizard to specify the file, folder or all drives in a system that are to be audited. You can also edit existing templates, copy templates, disable/enable templates, or remove templates that are no longer being used.

> **i** | **NOTE:** For more information, including a full description of the page, refer to the Quest Change Auditor for Windows File Server User Guide.

To create an auditing template for a file:

1   Open the Administration Tasks page.

2   Click **Auditing**.

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

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

Table 38. File System Auditing Wizard: File auditing

Page	Description	Procedure
Welcome	Name your template.	1 Enter a name for the template. 2 Click **Next**.
File Paths	Provide the name and path of the files to be audited. Use the Events tab to select vital file events. This must be a local path. Auditing and/or protecting network shares is not supported. To audit or protect those files/folders, a Change Auditor agent must be deployed on the share's hosting server.	1 For the audit path, select **File**. 2 Enter the file name and path (i.e., *Drive:\Folder\FileName.ext*) to be audited. 3 Click **Add** to add it to the selection list. 4 On the Events tab, select individual file events to be audited, or select the **File Events** check box to select all listed file events. 5 Click **Next**.
Excluded Processes	(Optional) Select the processes to exclude from auditing.	1 Enter a process to exclude 2 Click **Add** to add it to the exclusion list. 3 Repeat to add additional processes. 4 Click **Finish** to save the template and close the wizard.

To create an auditing template for a folder/all drives:

1   Open the Administration Tasks page.

2   Click **Auditing**.

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

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

Table 39. File System Auditing Wizard: Folder/All Drives auditing

Page	Description	Procedure
Welcome	Name your template.	1 Enter a name for the template. 2 Click **Next**.

Table 39. File System Auditing Wizard: Folder/All Drives auditing

Page	Description	Procedure
File Paths	Provide the name and path of the folders to be audited or select to audit all drives. Use the available tabs to select specific events and file masks to audit. You can also exclude certain subfolders and files from auditing. **NOTE:** This must be a local path. Auditing and/or protecting network shares is not supported. To audit or protect those files/folders, a Change Auditor agent must be deployed on the share's hosting server. **NOTE:** Do not use the Inclusion tab to add additional subfolder paths onto the monitored base path (audit path specified above). It is meant to specify an inclusion mask for ONLY objects located under the monitored base path. **IMPORTANT:** If you enter the name of a subfolder or file that is outside of the audited path, it will NOT be excluded from auditing. **NOTE:** For file system auditing, the slash characters (\) and double asterisks (**) are not allowed in file masks; therefore, to include a specific folder (or share), use the Audit Path field at the top of the page to specify the folder (or share) to be audited and enter an * on the Inclusions tab.	1 For the audit path, select **Folder** or **All Drives**. ▪ If **Folder** is selected, enter the file name and path to be audited. You can also select a system variable using the drop-down menu. ▪ If **All Drives** is selected, the **Audit Path** text box will contain an asterisk (*) which cannot be changed. Click **Add** to add it to the selection list. 2 Click in the **Scope** cell to change the scope of coverage. 3 On the Events tab, select individual file and folder events to be audited, or select the **File Events** and/or **Folder Events** check boxes to select all listed events. 4 On the Inclusions tab, enter a file mask to specify what is to be included in the audit using the following: ▪ Fixed characters such as letters, numbers and other characters that are allowed in file names. ▪ Asterisk (*) wildcard character to substitute zero or more characters. ▪ Question mark (?) wildcard character to substitute a single character. Click **Add** to add it to the inclusion list. 5 (Optional) On the Exclusions tab, specify the names and paths of any subfolders or files to exclude. 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. Use **Add	Folder** to exclude activity against any matching files/subfolders or **Add	File** to exclude activity against matching files.

Table 39. File System Auditing Wizard: Folder/All Drives auditing

Page	Description	Procedure
Discarded events	(Optional) Multiple folder open events are generated by tooltips (folder content information that is displayed when you hover your mouse over a folder) because Windows Explorer navigates the folder tree for all the sub-folders when you hover over the parent folder to see the tooltip. (Optional) Multiple folder open events are generated by file scans because Windows Explorer opens and reads the header of all files contained in an opened folder for information to display in the window.	1 To ignore the folder opened events generated by this action, select the **Discard Windows Explorer tooltip events from browsing** option. 2 To ignore the folder open events generated by this action, select the **Discard file open events from folder browsing** option. 3 Click **Next**. **NOTE:** Clicking **Finish** saves the template and closes the wizard.
Excluded Processes	(Optional) Select the processes to exclude from auditing.	1 Enter a process to exclude and click **Add** to add it to the exclusion list. Repeat to add additional processes. 2 Click **Finish** to save the template and close the wizard.

Registry auditing

To capture registry events, you must first complete the following steps to define the registry keys to be audited and the events to be captured:

1 Create a Registry Auditing template which specifies the registry key(s) and events to be audited.

2 Add this template to an agent configuration. (See Define agent configurations.)

3 Assign the agent configuration to agents. (See Assign agent configurations to agents.)

Registry Auditing page

The Registry Auditing page is displayed when **Registry** is selected from the Auditing task list in the navigation pane of the Administration Tasks page, and contains an expandable view of all the Registry Auditing templates that have been previously defined. From this page you can launch the Registry Auditing wizard to specify a registry key to be audited. You can also edit existing templates, copy templates, disable/enable templates, or remove templates that are no longer being used.

i | **NOTE:** For more information, including a full description of the page, refer to the Change Auditor User Guide.

To create a Registry Auditing template:

1 Open the Administration Tasks page.

2 Click **Auditing**.

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

4 Click **Add** to open the Registry Auditing wizard which steps you through the process of creating a Registry Auditing template.

Table 40. Registry Auditing Wizard

Page	Description	Procedure
Welcome	Name your template.	1 Enter a name for the template. 2 Click **Next**.
Registry Key Selection	Select the registry keys to be audited. Use the Event tab to select any associated events that are to be audited. Use the Exclusions tab to specify sub keys to be excluded.	1 Enter the registry in the HKEY_LOCAL_MACHINE hive to be audited and click **Add** to add it to the selection list. 2 To change the default scope, click the entry in the **Scope** cell and select a different scope. 3 On the Events tab, select the key and value events that are to be included in the audit. Selecting the **Key Events** or **Value Events** check box selects all of the events underneath the heading. 4 If you selected **This object and child objects only** as the scope, on the Value tab you can specify a specific value for the selected key. 5 (Optional) On the Exclusions tab, add the names of any sub keys to be excluded from auditing. Only the names of sub keys that belong to the selected registry key should be entered. Or use a file mask to select a group of sub keys. A file mask can contain any combination of the following: ▪ Fixed characters such as letters, numbers and other characters allowed in sub key names. ▪ Asterisk (*) wildcard character to substitute zero or more characters. ▪ Question mark (?) wildcard character to substitute a single character. Click **Add** to add it to the Exclusion list at the bottom of the page. 6 Click **Finish** to save the template and close the wizard.

Services auditing

To capture service events, you must first complete the following steps to define the services to be audited:

1 Create a Service Auditing template which specifies the system server(s) to be audited or excluded from auditing.

2 Add this template to an agent configuration. (See Define agent configurations.)

3 Assign the agent configuration to Change Auditor agents. (See Assign agent configurations to agents.)

Services Auditing page

The Services Auditing page is displayed when **Services** is selected from the Auditing task list in the navigation pane of the Administration Tasks page, and contains an expandable view of all the Service Auditing templates that have been previously defined. From this page you can launch the Service Auditing wizard to define the system services to be included in the auditing template. You can also edit existing templates, copy templates, disable/enable templates, or remove templates that are no longer being used.

> **i** | **NOTE:** For more information, including a full description of the page, refer to the Change Auditor User Guide.

To create a Service Auditing template:

1 Open the Administration Tasks page.

2 Click **Auditing**.

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

4 Click **Add** to open the Service Auditing wizard which allows you to define the system services to be included in the template.

Table 41. Service Auditing Wizard

Page	Description	Procedure
Welcome	Name your template.	1 Enter a name for the template. 2 Click **Next**.
Services Selection	Select the system services to be included in or excluded from auditing. By default, all services will be audited.	1 Select one of the following options to define whether this template is to include or exclude system services for auditing: ▪ **Audit ALL services** ▪ **Audit ALL services except the following** ▪ **Audit ONLY the following services** 2 If you selected either **Audit ALL services except the following** or **Audit ONLY the following services**, enter the names of the services to be included/excluded and click **Add** to add them to the selection list. 3 Click **Finish** to save the template and close the wizard.

NAS

The tasks under this heading are used to create auditing templates for NAS devices. After creating an EMC, Fluid File System, or NetApp auditing template, see Templates with defined agents for information on immediately enabling the auditing defined in these templates.

See the following administration task descriptions for more information:

- EMC auditing
- NetApp auditing
- Fluid File System (FluidFS) auditing

EMC auditing

To enable EMC auditing, you must first create an EMC Auditing template for each EMC file server (CIFS) to be audited. Each auditing template defines the location of the EMC file server to be audited, the auditing scope, and the Change Auditor agents that are to receive the EMC events.

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

EMC Auditing page

The EMC Auditing page is displayed when **EMC** is selected from the Auditing task list in the navigation pane of the Administration Tasks page, and contains an expandable view of all the EMC Auditing templates that have been previously defined. From this page you can launch the EMC Auditing wizard to specify the EMC file server (CIFS) to be audited, the auditing scope and the agents that are to receive the EMC events. You can also edit existing templates, disable/enable templates, and remove templates that are no longer being used.

> **i** | **NOTE:** For more information, including a full description of the page, refer to the Quest Change Auditor for EMC User Guide.

To audit a file:

1   Open the Administration Tasks page.

2   Click **Auditing**.

3   Select **EMC** (under the NAS heading in the Auditing task list) to open the EMC Auditing page.

4   Click **Add** to launch the EMC Auditing wizard.

Table 42. EMC Auditing Wizard: File auditing

Page	Description	Procedure
Welcome	Specify the EMC File Server (CIFS) to be audited.	1 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. 2 Click **Next**.
File Path Selection (File)	Provide the name and path of a file(s) to be audited. Use the Events tab to select vital file events.	1 For the audit path, select **File**. 2 Enter the file name and path (i.e., *<ShareName>\<Path>\<FileName>*) to be audited. **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. 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 "Isilon admin share name" link on the top right corner of the page. 3 Click **Add** to add it to the selection list. 4 On the Events tab, select individual file events to be audited or select the **File Events** check box to select all listed file events. 5 Click **Next**.

Table 42. EMC Auditing Wizard: File auditing

Page	Description	Procedure

Agent Selection	Select the Change Auditor agents to be used to monitor the EMC file server.
	
	 If the Change Auditor agents are not already specified in the cepp.conf file (pool namesakes servers entry), use **Set Credentials** to provide the credentials and create the cepp.conf file.
		1 Click **Add** to open the Eligible Change Auditor Agents dialog.
		
		 2 Select one or more agents from the list.
		
		 3 Click **OK** and continue to Step 8. If the list appears empty, click **Cancel** to return to the Agent Selection page.
		
		 4 If there are no Change Auditor agents available on the Eligible Change Auditor Agents dialog, click **Set Credentials** and enter the following information:
		
		   ▪ **Control Station** - IP address of the EMC Control Station.
		
		   ▪ **User** - user name of an account with Administrative rights on the EMC Control Station.
		
		   ▪ **Password** - password associated with the user name.
		
		   ▪ **Data Mover** - use the drop-down to select the Data mover that hosts the CIFS file server specified on the first wizard page.
		
		 5 Click **Test** to validate the credentials. Once the credentials have been validated, click **OK**.
		
		 6 Click **Add** to open the Eligible Change Auditor Agents dialog.
		
		 7 Select one or more agents from the list. Click **OK**.
		
		 8 Click **Next**.

Configuration	Review the proposed cepp.conf file. (Optional) From this page you can also deploy the proposed configuration file, check the status of the cepp service and audit the cepp.conf file.	1 Review the proposed cepp.conf file. 2 (Optional) Click **Update File** to deploy the proposed configuration file on the EMC Control Station. 3 (Optional) Click **Check Status** to check the status of the cepp service. 4 (Optional) Click **Audit File** to enable/disable the auditing of the cepp.conf file for changes made to this configuration file by third-party applications. 5 Click **Finish** to save the template and close the wizard.

To audit a folder or volume:

1 Open the Administration Tasks page.

2 Click **Auditing**.

3 Select **EMC** (under the NAS heading in the Auditing task list) to open the EMC Auditing page.

4 Click **Add** to open the EMC Auditing wizard.

Table 43. EMC Auditing Wizard: Folder/Volume auditing

Page	Description	Procedure
Welcome	Specify the EMC File Server (CIFS) to be audited.	1 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. 2 Click **Next**.

Table 43. EMC Auditing Wizard: Folder/Volume auditing

Page	Description	Procedure
File Path Selection (Folder/Volume/ All Volumes)	Provide the name and path of a folders/volumes to be audited. Use the available tabs to select specific events and file masks to audit. You can also exclude certain subfolders and files from auditing. **NOTE:** Volume names are case sensitive. **IMPORTANT:** If you enter the name of a subfolder or file that is outside of the audited path, it will NOT be excluded from auditing.	1 For the audit path, select **Folder**, **Volume** or **All Volumes**. 2 If **Folder** is selected, enter the folder name and path (*<ShareName>\<FolderName>*) to audit, and click **Add**. 3 If **Volume** is selected, enter a volume name (*<VolumeName>*), and click **Add**. 4 If **All Volumes** is selected, click **Add** to add all volumes. 5 Click in the **Scope** cell to change the scope of coverage. 6 On the Events tab, select individual file and folder events to audit, or select the **File Events** and **Folder Events** check boxes to select all listed events. 7 On the Inclusions tab, enter a file mask to specify what is to be included in the audit using 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. Click **Add** to add it to the inclusion list. 8 (Optional) On the Exclusions tab, specify the names and paths of any subfolders or files to exclude. 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. Use **Add	Folder** to exclude activity against any matching files/subfolders or **Add	File** to exclude activity against matching files. 9 Click **Next**.

Table 43. EMC Auditing Wizard: Folder/Volume auditing

Page	Description	Procedure

Agent Selection	Select the agents to be used to monitor the EMC file server.
	
	If the Change Auditor agents are not already specified in the cepp.conf file (pool name=quest servers entry), you will need to provide credentials.
		1 Click **Add** to open the Eligible Change Auditor Agents dialog.
		
		2 Select one or more agents from the list.
		
		3 Click **OK** and continue to Step 8. If the list appears empty, click **Cancel** to return to the Agent Selection page.
		
		4 If there are no agents available on the Eligible Change Auditor Agents dialog, click **Set Credentials** and enter the following information:
		
		  ▪ **Control Station** - IP address of the EMC Control Station.
		
		  ▪ **User** - user name of an account with Administrative rights on the EMC Control Station.
		
		  ▪ **Password** - password associated with the user name.
		
		  ▪ **Data Mover** - use the drop-down to select the Data mover that hosts the CIFS file server specified on the first wizard page.
		
		5 Click **Test** to validate the credentials. Once the credentials have been validated, click **OK**.
		
		6 Click **Add** to open the Eligible Change Auditor Agents dialog.
		
		7 Select one or more agents from the list. Click **OK**.
		
		8 Click **Next**.

Configuration	Review the proposed cepp.conf file. (Optional) From this page you can also deploy the proposed configuration file, check the status of the cepp service and audit the cepp.conf file.	1 Review the proposed cepp.conf file. 2 (Optional) Click **Update File** to deploy the proposed configuration file on the EMC Control Station. 3 (Optional) Click **Check Status** to check the status of the cepp service. 4 (Optional) Click **Audit File** to enable/disable the auditing of the cepp.conf file for changes made to this configuration file by third-party applications. 5 Click **Finish** to save the template and close the wizard.

NetApp auditing

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

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

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

¡ | **NOTE:** NetApp events initiated through the NFS protocol are not supported.

NetApp Auditing page

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

¡ | **NOTE:** For more information, including a full description of the page, refer to the Quest Change Auditor for NetApp User Guide.

To audit a file:

1 Open the Administration Tasks page.

2 Click **Auditing**.

3 Select **NetApp** (under the NAS heading in the Auditing task list) to open the NetApp Auditing page.

4 Click **Add** to open NetApp Auditing wizard.

Table 44. NetApp Auditing Wizard: File auditing

Page	Description	Procedure

Welcome	Specify the NetApp filer to be audited.	1 Select the NetApp CIFS server from the drop-down menu. If the NetApp CIFS server not appear in the list, enter the server's NetBIOS name.
		
		2 File and folder auditing is supported in both 7-mode (non-cluster mode) and cluster mode. Select **Detect filer mode** to determine which mode you have deployed.
		
		  If you are operating in cluster mode, credentials must be set for all agents. The credentials set must be for users with ONTAPI access on the filer. Enter the credentials and click **OK**.
		
		  Once entered, Change Auditor verifies that the specified account can access the filer. If there is an issue, re-enter valid credentials and the verification will run again.
		
		3 Click **Next**.

Table 44. NetApp Auditing Wizard: File auditing

Page	Description	Procedure
File Path Selection (File)	Provide the name and path of a files to be audited. Use the Events tab to select vital file events.	1 For the audit path, select **File**. 2 Enter the file name and path (*<ShareName>**<Path>**<FileName>*) to audit and click **Add** to add it to the selection list. 3 On the Events tab, select individual file events to be audited or select the **File Events** check box to select all listed file events. 4 Click **Next**.
Agent Selection	Select the Change Auditor agents to be used to monitor the NetApp filer test. (Optional) Supply NetApp filer credentials.	1 Click **Add** to open the Eligible Change Auditor Agents dialog. Select the agents to be used. (Use the **Shift** or **Ctrl** keys to select multiple agents.) Click **OK** to close the dialog and add the agents to the selection list. 2 (Optional) If you did NOT add the agent accounts to the local Administrators group on the NetApp filer, select the agent from the list and click **Set Credentials** to enter the NetApp filer credentials. Click **Clear Credentials** to clear any previously entered NetApp filer credentials for the selected agent. 3 Click **Finish** to save the template and close the wizard.

To audit a folder/volume:

1   Open the Administration Tasks page.

2   Click **Auditing**.

3   Select **NetApp** (under the NAS heading in the Auditing task list) to open the NetApp Auditing page.

4   Click **Add** to open the NetApp Auditing wizard.

Table 45. NetApp Auditing Wizard: Folder/Volume auditing

Page	Description	Procedure
Welcome	Specify the NetApp filer to be audited.	1 Select the NetApp CIFS server from the drop-down menu. If the NetApp CIFS server not appear in the list, enter the server's NetBIOS name. 2 Click **Next**.

Table 45. NetApp Auditing Wizard: Folder/Volume auditing

Page	Description	Procedure
File Path Selection (Folder/ Volume/ All Volumes)	Provide the name and path of a folders/volumes to be audited. Use the available tabs to select specific events and file masks to audit. You can also exclude certain subfolders and files from auditing. **NOTE:** Volume names are case sensitive. **IMPORTANT:** If you enter the name of a subfolder or file that is outside of the audited path, it will NOT be excluded from auditing. **NOTE:** The slash (\) and double asterisk (**) characters can only be used with volumes.	1 For the audit path, select **Folder**, **Volume** or **All Volumes**. 2 If **Folder** is selected, enter the folder name and path (*<ShareName>\<FolderName>*) to audit and click **Add**. 3 If **Volume** is selected, enter a volume (*<VolumeName>*) and click **Add**. 4 If **All Volumes** is selected, click **Add**. 5 Click in the **Scope** cell to change the scope of coverage. 6 On the Events tab, select individual file and folder events to be audited, or select the **File Events** and **Folder Events** check boxes to select all listed events. 7 On the Inclusions tab, enter a file mask to specify what is to be included in the audit using 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). Click **Add** to add it to the inclusion list. 8 (Optional) On the Exclusions tab, specify the names and paths of any subfolders or files to exclude. 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. Use **Add	Folder** to exclude activity against any matching files/subfolders or **Add	File** to exclude activity against matching files. 9 Click **Next**.

Table 45. NetApp Auditing Wizard: Folder/Volume auditing

Page	Description	Procedure
Agent Selection	Select the agents to be used to monitor the NetApp filer test. (Optional) Supply NetApp filer credentials.	1 Click **Add** to open the Eligible Change Auditor Agents dialog. Select the agents to be used. (Use the **Shift** or **Ctrl** keys to select multiple agents.) Click **OK** to close the dialog and add the agent(s) to the selection list. 2 (Optional) If you did NOT add the agent accounts to the local Administrators group on the NetApp filer, select the agent from the list and click **Set Credentials** to enter the NetApp filer credentials. Click **Clear Credentials** to clear any previously entered NetApp filer credentials for the selected agent. 3 Click **Finish** to save the template and close the wizard.

Fluid File System (FluidFS) auditing

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

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

> **NOTE:** Auditing is supported only for the CIFS/SMB protocol. Events initiated through the NFS or FTP protocols are not supported.

Before you begin:

- Verify that Dell Enterprise Manager (and Data Collector service) is properly installed and configured.
- Verify that the FluidFS cluster you plan to audit is registered with Enterprise Manager.
- Ensure you have Administrator rights to Enterprise Manager.
- Ensure that the Change Auditor Configuration Service for Dell FluidFS is installed.

For installation and configuration details, see the Change Auditor for Fluid File System User Guide.

FluidFS Auditing page

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

> **NOTE:** For more information, including a full description of the page, refer to the Quest Change Auditor for Fluid File System User Guide.

To audit a file:

1 Open the Administration Tasks page.

2 Click **Auditing**.

3 Select **FluidFS** (under the NAS heading in the Auditing task list) to open the FluidFS Auditing page.

4 Click **Add** to open the Auditing wizard.

Table 46. FluidFS Auditing Wizard

Page	Description	Procedure
Welcome	Specify the FluidFS cluster to be audited, and the credentials required to configure auditing.	1 Enter or select the FluidFS cluster name from the drop-down list to be audited. **NOTE:** The drop-down list contains the clusters published in Active Directory. **NOTE:** IP Addresses are not supported at this time. To select a volume to be audited, you will need to enter the Change Auditor Configuration Service for Dell FluidFS location and an account that has administrative privileges to access Enterprise Manager. This allows the Coordinator to connect with the service and populate the list of available volumes to audit. 2 Click the **Provide FluidFS Credentials** button to be prompted for the credentials. The credentials are case sensitive. 3 Click **Next**.

Table 46. FluidFS Auditing Wizard

Page	Description	Procedure
File Path Selection	Provide the name and path of a volume to be audited. Use the available tabs to select specific events and file masks to audit. You can also exclude certain subfolders and files from auditing. Use the Events tab to select vital events.	4 Enter the volume to audit and click **Add** to add it to the selection list. 5 On the Events tab, select individual file and folder events to be audited, or select the **File Events** and **Folder Events** check boxes to select all listed events. 6 On the Inclusions tab, enter a file mask to specify what is to be included in the audit using 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). 7 Click the **Add** button to add it to the Included Names list. 8 On the Exclusions tab, specify the names and paths of any subfolders or files to exclude. 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. 9 Click **Add and select File or Folder** to add it to the exclusions list. 10 Click **Next**.

Table 46. FluidFS Auditing Wizard

Page	Description	Procedure
Agent Selection	Select the agents to be used to monitor the cluster. **NOTE:** The domain of the configuration service must have a two-way trust with the domain of the auditing agent and trust the domain of the coordinator (one-way trust).	11 Click **Add** to open the Change Auditor Agents dialog. Select the agents to be used. 12 Click **OK** to close the dialog and add the agents to the selection list.
Encryption Settings	Turn encryption on to protect the data as it passes between the FluidFS cluster and the agents. **NOTE:** Encryption settings are not maintained when a template is exported. You will need to re-configure this setting on any previously deleted templates after it has been imported. **NOTE:** The domain of the coordinator must trust the domain of the specified user account (one-way trust).	13 To enable encryption, select **Turn on encryption for auditing**, click the **Set credentials for encryption**, and enter the service account credentials for the FluidFS cluster to use when encrypting events. When required, you can turn off the encryption through the Enterprise Manager client. If you turn off encryption, you need to refresh Change Auditors' configuration so that it is synchronized with the FluidFS cluster. To refresh the configuration, save the FluidFS template after the change or run the Update-CAFluidFSConfiguration command. The FluidFS.Configuration.Service.PowerShell module is located in the install directory of the Change Auditor Configuration Service for Dell FluidFS. 14 Click **Finish** to save the template and close the wizard.

Protection Tasks (Administration Tasks Page)

- Introduction
- Forest
- Application
- Server

Introduction

Protection enables administrators to lock down critical objects and attributes to prevent accidental or unauthorized creations, modifications, deletions, and access. This allows you to protect the environment from harmful changes that could open security holes or cause resources to become unavailable.

The protection task list is divided into the following separate task lists:

- Forest
  - Active Directory object protection
  - ADAM (AD LDS) object protection
  - Group Policy object protection
- Application
  - Exchange Mailbox protection
- Server
  - File System protection

ℹ **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 any of these pages, see Application User Interface Authorization page for information.

Forest

With Change Auditor for Active Directory, you can protect any Active Directory, Group Policy, or ADAM (AD LDS) objects that you consider critical. Examples of such objects may include Organizational Units, Group Policy Objects, and service accounts.

ℹ **NOTE:** For more information, including recommendations and full descriptions of the following protection pages, see the Quest Change Auditor for Active Directory User Guide.

See the following administration task descriptions for more information:

- Active Directory object protection

- ADAM (AD LDS) object protection
- Group Policy object protection

Active Directory object protection

When configured, Change Auditor prevents changes from occurring to a protected object regardless of who attempts to change the object and the tool or method used. Attempts to change or delete a protected object fail and an event is generated. These 'failed' events are identified by displaying 'Protected' in the **Result** column on the Search Results page and **Result** field in an event's detail pane.

i | **NOTE:** See the Quest Change Auditor User Guide for information about defining the events to capture based on result.

Active Directory Protection page

The Active Directory Protection page is displayed when **Active Directory** is selected from the Protection task list in the navigation pane of the Administration Tasks page, and contains an expandable view of all the Active Directory Protection templates that have been previously defined. From this page, you can open the Active Directory Protection wizard to define critical Active Directory objects to protect from unauthorized modifications. You can also edit existing templates, disable and enable templates, and remove templates that are no longer required.

The Active Directory protection templates defined on the Active Directory Protection page are global settings and apply to all agents.

i | **NOTE:** If you are planning to use multiple Active Directory Protection templates, see the Quest Change Auditor Technical Insight Guide for more information about how multiple protection templates are evaluated.

To create an Active Directory Protection template:

1 Open the Administration Tasks page.

2 Click **Protection**.

3 Select **Active Directory** in the Protection task list to open the Active Directory Protection page.

4 Click **Add** to open the Active Directory Protection wizard which allows you to specify the Active Directory objects to be protected.

Table 47. Active Directory Protection wizard

Page	Description	Procedure
Welcome	Name your template.	1 Enter a name for the template. 2 Click **Next**.
Object Selection	Use the Browse or Search page to locate and select the directory objects to protect. See Directory object picker for a detailed description of this wizard page.	1 From the Browse or Search page, select an object and click **Add** to add it to the selection list at the bottom of the page. 2 To change the default operations, click the entry in the **Operations** cell and select or clear operations. 3 To change the default scope, click the entry in the **Scope** cell and select a different scope. 4 Click **Next**. **NOTE:** Clicking **Finish** saves the template and closes the wizard.

Table 47. Active Directory Protection wizard

Page	Description	Procedure

Attribute Protection	(Optional) Specify the attributes to include and exclude.
	
	By default, all attributes for the selected objects are protected.
		1 To protect individual attributes instead of all attributes, select one of the following options:
		
		  ▪ **Only Selected**
		
		  ▪ **All EXCEPT Selected**
		
		2 From the attribute list on the left, select the individual attributes to included and click **Add** to move them to the Selected Attributes list on the right.
		
		3 Click **Next**.
		
		NOTE: Clicking **Finish** saves the template and closes the wizard.

Schedule when protection is enabled	(Optional) Schedule when the protection is enforced. You can either select to have the protection always run or have it run only during specific times. The times selected are the local agent time where the template is applied. **NOTE:** If you have denied specific users or groups the ability to change the protected objects and you have enabled a protection schedule, those users or groups are denied access only during this time. Anytime outside of when the schedule is set to enabled, these denied accounts can access the protected object. When the schedule is disabled, all options are disabled with it, including any denied access to the specified users. The scheduling options override all other protection settings.	1 To enable the protection only during specific times, select the Protection is scheduled option, and define when it should be enabled (hour blocks on a weekly basis). 2 Click **Next**.

Enable or disable protection for specific location	(Optional) Control when the protection is enabled based on the location.
	
	Location refers to the computer that is attempting to access the resource that is protected.
	
	NOTE: If you have denied specific users or groups access to protected objects, but you have specified locations that an access the protected object, the denied user or group can access the protected objects from these locations.
	
	The location options override all other protection settings.
		1 Select from the following options:
		
		  ▪ **Protect access from all locations**: Protection is always enabled regardless of the location.
		
		  ▪ **Protect access only from select locations**: Protection is only enabled for the locations specified in the list box.
		
		  ▪ **Allow access only from select locations**: Protection is disabled for the select locations. Enabled everywhere else.
		
		  ▪ **Protect access from all unknown locations**: All file system requests from locations that cannot be determined by the agent will be protected.
		
		2 Click **Next**.

Table 47. Active Directory Protection wizard

Page	Description	Procedure
Account Access	(Optional) Specify the accounts that are allowed to change the protected objects. By default all users and groups are prevented from changing the Active Directory objects selected for protection.	1 Select whether to **Allow** or **Deny** access for the selected users or groups. Keep in mind that by selecting **Deny**, you are allowing all users to change the protected object EXCEPT for those selected on this page. 2 From the Browse or Search page, select an object and click **Add** to add it to the selection list at the bottom of the page. 3 Click **Next**. **NOTE:** Clicking **Finish** saves the template and closes the wizard.
Template Management	(Optional) Specify individual users or groups who are authorized to manage this protection template. **NOTE:** This page only appears when your Active Directory and Group Policy protection templates are stored in SQL, which is the default location for storing these templates. **IMPORTANT:** Edits made on this page impact template access rights. For more information about this protection feature, see the Quest Change Auditor User Guide.	1 From the Browse or Search page, select an account and click **Add** to add it to the selection list at the bottom of the page. 2 Click **Finish** to save the protection template and close the wizard. **IMPORTANT:** If the current user who is creating the protection template is not in the authorized accounts list, a warning message is displayed prompting the user to continue or stop with the creation of the protection template. If you are in the authorized accounts list at template creation time, you may be locked out later if someone else in the authorized accounts list edits the template and removes you.

ADAM (AD LDS) object protection

When configured, Change Auditor for Active Directory prevents changes to objects in specified ADAM (AD LDS) instances.

ADAM (AD LDS) Protection page

The ADAM (AD LDS) Protection page is displayed when **ADAM (AD LDS)** is selected from the Protection task list in the navigation pane of the Administration Tasks page, and contains an expandable view of all the ADAM (AD LDS) Protection templates that have been previously defined. From this page, you can open the ADAM (AD LDS) Protection wizard to define critical objects to protect from unauthorized modifications. You can also edit existing templates, disable and enable templates, and remove templates that are no longer required.

The ADAM (AD LDS) protection templates defined on this page are global settings and apply to all ADAM instances associated with a Change Auditor agent.

i | **NOTE:** If you are planning to use multiple ADAM (AD LDS) Protection templates, see the Quest Change Auditor Technical Insight Guide for more information about how multiple protection templates are evaluated.

To create an ADAM (AD LDS) Protection template:

1   Open the Administration Tasks page.

2   Click **Protection**.

3   Select **ADAM (AD LDS)** in the Protection task list to open the ADAM (AD LDS) Protection page.

4   Click **Add** to open the ADAM (AD LDS) Protection wizard which allows you to specify the objects to be protected.

Table 48. ADAM (AD LDS) Protection wizard

Page	Description	Procedure
ADAM (AD LDS) Instance	Select the ADAM (AD LDS) instance from which to choose protected objects. The list displays the ADAM (AD LDS) instances discovered in your environment. Only instances running on computers with a Change Auditor agent installed are available.	1 Select the ADAM (AD LDS) instance from which to choose protected objects. 2 Enter the credentials for a Windows or ADAM/AD LDS account that can access the instance. 3 Click **Test** to verify the credentials and enable the **Next** button. If the credentials were incorrect, an error message is displayed. 4 Click **Next**. **NOTE:** If you have multiple ADAM (AD LDS) instances with replicating application partitions, there is no need to configure an auditing template for each instance. Change Auditor sends the auditing configuration to each computer that is hosting an instance. You must have an agent installed on each instance host
Welcome	Name your template.	1 Enter a name for the template. 2 Click **Next**.

Table 48. ADAM (AD LDS) Protection wizard

Page	Description	Procedure
Object Selection	Use the Browse or Search page to locate and select the objects to protect. See Directory object picker for a detailed description of this wizard page.	1 From the Browse or Search page, select an object to protect and click **Add**. 2 To change the default operations, click the entry in the **Operations** cell and select or clear operations. 3 To change the default scope, click the entry in the **Scope** cell and select a different scope. 4 Click **Next**. **NOTE:** Clicking **Finish** saves the template and closes the wizard.
Attribute Protection	(Optional) Specify the attributes to include and exclude. By default, all attributes for the selected objects are protected.	1 To protect individual attributes, select one of the following options: ▪ **Only Selected** ▪ **All EXCEPT Selected** 2 From the attribute list on the left, select the individual attributes to include and click **Add** to move them to the Selected Attributes list on the right. 3 Click **Next**. **NOTE:** Clicking **Finish** saves the template and closes the wizard.
Account Access	(Optional) Specify the accounts that are allowed to change the protected objects. By default, all users and groups are prevented from changing the objects selected for protection.	1 Select whether to **Allow** or **Deny** access for the selected users or groups. Keep in mind that by selecting **Deny**, you are allowing all users to change the protected object except for those selected on this page. 2 From the Browse or Search page, select an object and click **Add** to add it to the selection list at the bottom of the page. 3 Click **Finish** to save the template and close the wizard.

Group Policy object protection

When configured, Change Auditor prevents all changes to GPOs, regardless of the tool that is used to make the change. Protection includes both portions of the Group Policy data: the Group Policy objects in Active Directory and the actual configuration data stored in the SYSVOL share on domain controllers.

> **IMPORTANT:** A protected Group Policy Object can only be changed by override accounts that are excluded from protection.

> **NOTE:** When an attempt is made to use the Windows Group Policy Editor to change a group policy object (that is protected by Change Auditor), an access-denied error is displayed indicating that the change was not saved. However, when the error is dismissed the unsaved change will still be shown in the Editor as if it had been saved because the Group Policy Editor will not automatically refresh. To show the true (unchanged) state of the group policy object, you must close and reopen the Editor.

Group Policy Protection page

The Group Policy Protection page is displayed when **Group Policy** is selected from the Protection task list in the navigation pane of the Administration Tasks page, and contains an expandable view of all the Group Policy Protection templates that have been previously defined. From this page, you can open the Group Policy Protection wizard to define critical group policy objects to protect from unauthorized modifications. You can also edit existing templates, disable and enable templates, and remove templates that are no longer being used.

The Group Policy protection templates defined on this page are global settings and apply to all Change Auditor agents.

> **i** | **NOTE:** If you are planning to use multiple Group Policy Protection templates, see the Quest Change Auditor Technical Insight Guide for more information about how multiple protection templates are evaluated.

To create a Group Policy Protection template:

1 Open the Administration Tasks page.

2 Click **Protection**.

3 Select **Group Policy** in the Protection task list to open the Group Policy Protection page.

4 Click **Add** to open the Group Policy Protection wizard which allows you to specify the group policy objects to be protected.

Table 49. Group Policy Protection wizard

Page	Description	Procedure
Welcome	Name your template.	1 Enter a name for the template. 2 Click **Next**.
Object Selection	Use the Browse or Search page to locate and select a group policy container to protect. See Directory object picker for a detailed description of this wizard page.	1 From the Browse or Search page, select a group policy container and click **Add**. *OR* To protect all group policy containers in the Enterprise, click the **Enterprise** button. 2 To change the default operations, click the entry in the **Operations** cell and select or clear operations. 3 Click **Next**. **NOTE:** Clicking **Finish** saves the template and closes the wizard.
Account Access	(Optional) Specify the accounts that are allowed to change the protected group policy object. By default all users and groups are prevented from changing the Group Policy containers selected for protection. **NOTE:** Management actions performed by excluded accounts are audited but not prevented.	1 Select whether to **Allow** or **Deny** access for the selected users or groups. Keep in mind that by selecting **Deny**, you are allowing all users to change the protected object EXCEPT for those selected on this page. 2 From the Browse or Search page, select an object and click **Add** to add it to the selection list at the bottom of the page. 3 Click **Next**. **NOTE:** Clicking **Finish** saves the template and closes the wizard.

Table 49. Group Policy Protection wizard

Page	Description	Procedure
Template Management	(Optional) Specify individual users or groups who are authorized to manage this protection template. **NOTE:** This page only appears when your Active Directory and Group Policy protection templates are stored in SQL, which is the default location for storing these templates. **IMPORTANT:** Edits made on this page impact template access rights. For more information about this protection feature, see the Quest Change Auditor User Guide.	1 From the Browse or Search page, select an account and click **Add** to add it to the selection list at the bottom of the page. 2 Click **Finish** to save the protection template and close the wizard. **IMPORTANT:** If the current user who is creating the protection template is not in the authorized accounts list, a warning message is displayed prompting the user to continue or stop with the creation of the protection template. If you are in the authorized accounts list at template creation time, you may be f locked out later if someone else in the authorized accounts list edits the template and remove you.

Application

When licensed, Change Auditor for Exchange can provide extra protection over important mailboxes. The Exchange Mailbox protection prevents unwanted access to Exchange mailboxes, making it much more difficult for rogue administrators to access critical mailboxes.

Protection prevents users from accessing a mailbox through Outlook client; it does not prevent accessing a protected mailbox using OWA, ActiveSync, and EWS or changing permission on the mailbox through the Exchange Administration tools

See the Exchange Mailbox protection description for more information.

Exchange Mailbox protection

To enable Exchange Mailbox protection, you must first create one or more Exchange Mailbox Protection templates which specify whose mailboxes to lock down. Once Exchange Mailbox Protection templates are defined, they apply to all Exchange servers that host a Change Auditor agent.

> **i** | **NOTE:** If you are planning to use multiple Exchange Mailbox Protection templates, see the Quest Change Auditor Technical Insight Guide for more information about how multiple protection templates are evaluated.

> **i** | **NOTE:** For more information, including tips for improving process speed and full descriptions of the following protection page, see the Quest Change Auditor for Exchange User Guide.

Exchange Mailbox Protection page

The Exchange Mailbox Protection page opens when **Exchange Mailbox** is selected from the Protection task list in the navigation pane of the Administration Tasks page, and contains an expandable view of all the Exchange Mailbox Protection templates that have been previously defined. From this page, you can open the Exchange Mailbox Protection wizard to define whose mailboxes to protect from unauthorized access. You can also edit existing templates, disable and enable templates, and remove templates that are no longer being used.

To create an Exchange Mailbox Protection template:

1 Open the Administration Tasks page.

2 Click **Protection**.

3 Select **Exchange Mailbox** in the Protection task list to open the Exchange Mailbox Protection page.

4 Click **Add** to open the Exchange Protection wizard which steps you through the process of defining the mailboxes to protect.

Table 50. Exchange Protection wizard

Page	Description	Procedure
Welcome	Name your template.	1 Enter a name for the template. 2 Click **Next**.
Mailboxes	Use the Browse or Search page to locate and select the directory objects whose mailbox is to be protected. See Directory object picker for a detailed description of this wizard page.	1 From the Browse or Search page, select a directory object to protect and click **Add**. *OR* To protect all mailboxes in the Enterprise from unauthorized access, click **Enterprise**. 2 Click **Next**. **NOTE:** Clicking **Finish** saves the template and closes the wizard.
Account Access	(Optional) Specify the accounts that are allowed access to the selected protected mailboxes. By default, all users and groups are prevented from changing the objects selected for protection and mailbox owners can bypass protection to access their mailbox.	1 Select to either **Allow** or **Deny** access for the selected users or groups. Keep in mind that by selecting **Deny**, you are allowing all users to change the protected object EXCEPT for those selected on this page. 2 From the Browse or Search page, select a user or group account and click **Add** to add it to the selection list at the bottom of the page. 3 If you do not want mailbox owners to bypass protection and be able to access their own mailboxes, clear the **Mailbox owner can bypass protection** check box at the top of this page. 4 Click **Finish** to save the template and close the wizard.

Server

When licensed, Change Auditor for Windows File Servers provides enables administrators to secure business-critical files and folders on the file server against potentially dangerous changes.

> **i** | **NOTE:** For more information, including tips for improving performance and full descriptions of the following protection pages, see the Quest Change Auditor for Windows File Server User Guide.

See the File System protection task description for more information.

File System protection

To use File System protection, you must first complete the following steps to define the files and folders to protect:

1   Create a File System Protection template which specifies the files and folders to protect.

2   Add this template to an agent configuration. (See Define agent configurations.)

3   Assign the agent configuration to agents. (See Assign agent configurations to agents.)

The following sections go over the File System Protection page and how to create a File System Protection template.

File System Protection page

The File System Protection page opens when **File System** is selected from the Protection task list in the navigation pane of the Administration Tasks page, and contains an expandable view of all the File System Protection templates that have been previously defined. From this page, you can open the File System Protection wizard to specify a file or folder to protect from unauthorized access. You can also edit existing templates, disable and enable templates, and remove templates that are no longer being used.

> **i** | **NOTE:** If you are planning to use multiple File System Protection templates, see the Quest Change Auditor Technical Insight Guide for more information about how multiple protection templates are evaluated.

To create a File System Protection template:

1   Open the Administration Tasks page.

2   Click **Protection**.

3   Select **File System** in the Protection task list to open the File System Protection page.

4   Click **Add** to open the File System Protection wizard which steps you through the process of defining the files and folders to protect.

Table 51. File System Protection wizard

Page	Description	Procedure
Welcome	Name your template.	1 Enter a name for the template. 2 Click **Next**.

Table 51. File System Protection wizard

Page	Description	Procedure
File Path Selection	Specify the file system paths to protect. By default: • Protection is for the selected file system path. • Includes all subfolders. • Applies to both files and folders. • All types of protection (Read, Delete, Owner Change, and so on.) is applied. **NOTE:** This must be a local path. Auditing and protecting network shares is not supported. To audit or protect those files and folders, deploy an agent on the share's hosting server.	1 In the **Path** field, enter the file system path to protect and click **Add**. 2 To change the default protection to exclude the subfolders in the selected file system path, click the entry in the **Subfolders** cell and select **No**. 3 To change the default protection to exclude the selected file system from protection, click the entry in the **Protect** cell and select **No**. 4 To change the default protection of files and folders, click the entry in the **Applies To** cell and select a different option. 5 To change the default protection of all changes, click the entry in the **Protection Type** cell and select or clear protection types. 6 Use the **File Mask** field to optionally specify a file mask to protect a group of files in the selected file system path. Once you have specified a file mask, click **Add** to add it to the list at the bottom of the page. 7 Click **Next**. **NOTE:** Clicking **Finish** saves the template and closes the wizard.
Schedule when protection is enabled	(Optional) Schedule when the protection is enforced. You can either select to have the protection always run or have it run only during specific times. The times selected are the local agent time where the template is applied. **NOTE:** If you have denied specific users or groups the ability to change the protected objects and you have enabled a protection schedule, those users or groups are denied access only during this time. Anytime outside of when the schedule is set to enabled, these denied accounts can access the protected object. When the schedule is disabled, all options are disabled with it, including any denied access to the specified users. The scheduling options override all other protection settings.	1 To enable the protection only during specific times, select the Protection is scheduled option, and define when it should be enabled (hour blocks on a weekly basis). 2 Click **Next**.

Table 51. File System Protection wizard

Page	Description	Procedure
Enable or disable protection for specific location	(Optional) Control when the protection is enabled based on the location. Location refers to the computer that is attempting to access the resource that is protected. **NOTE:** If you have denied specific users or groups access to protected objects, but you have specified locations that can access the protected object, the denied user or group can access the protected objects from these locations. The location options override all other protection settings.	1 Select from the following options: ▪ **Protect access from all locations**: Protection is always enabled regardless of the location. ▪ **Protect access only from select locations**: Protection is only enabled for the locations specified in the list box. ▪ **Allow access only from select locations**: Protection is disabled for the select locations. Enabled everywhere else. ▪ **Protect access from all unknown locations**: All file system requests from locations that cannot be determined by the Change Auditor agent are protected. 2 Click **Next**.
Account Access	(Optional) Specify the user or group accounts which are allowed to change the protected objects selected on the previous page. By default, all users and groups are prevented from changing to the objects selected for protection.	1 Select to either **Allow** or **Deny** access for the selected users or groups. Keep in mind that by selecting **Deny**, you are allowing all users to change the protected objects except for those selected on this page. 2 From the Browse or Search page, select a user or group account and click **Add** to add it to the selection list at the bottom of the page. 3 Click **Finish** to save the template and close the wizard.

Change Auditor Client Comparison

The following table shows what Change Auditor features are available in the Change Auditor Windows client and Change Auditor web client.

Table 52. Change Auditor client comparison

Page/Feature	Available in Windows client?	Available in web client?
Overview Page	**Yes**	**Yes**
My Favorite Search	Yes	No
Overview Pane: Accounts Overview	No	Yes
Overview Pane: Agent Status: Enterprise	Yes	Yes
Overview Pane: Agent Status: Other	Yes	Yes
Overview Pane: Agent Status: Workstation	Yes	Yes
Overview Pane: Agent Status: *<Domain>*	Yes	Yes
Overview Pane: Alert History Counts	Yes: Alert History Counts	Yes: Alert History
Overview Pane: Alert History Counts by Query	Yes	Yes
Overview Pane: Coordinator Status: Enterprise	Yes	Yes
Overview Pane: Coordinator Status: *<Domain>*	Yes	Yes
Overview Pane: Count of Events by Event Class	Yes	Yes
Overview Pane: Count of Events by Facility	Yes	Yes
Overview Pane: Count of Events by Location	Yes	Yes
Overview Pane: Count of Events by Result	Yes	Yes
Overview Pane: Count of Events by Severity	Yes	Yes
Overview Panes: Count of Events by Subsystem	Yes	Yes
Overview Pane: File Access Rights	No	Yes
Overview Pane: File Ownership	No	Yes
Overview Pane: Recent Event Activity	Yes	Yes
Overview Pane: Top Agent Activity	Yes: Top Agent Activity	Yes: Agent Activity
Overview Pane: [Custom View]	No	Yes
Print page	Yes	No
Searches Page	**Yes**	**Yes**
Create New Folder	Yes	Yes
Create New Search	Yes	Yes
Run Search Query	Yes	Yes
Print page	Yes	No
Explorer/Folder View	Yes	Yes
Cut | Paste | Delete | Move | Copy Folder	Yes	Delete only
Rename Folder	Yes	Yes

Table 52. Change Auditor client comparison

Page/Feature	Available in Windows client?	Available in web client?
Export Folder	Yes	No
Import Search	Yes	No
Import Folder	Yes	No
Publish to Quest Knowledge Portal	Yes	No
Expand All | Collapse All	Yes	No
Searches List	Yes	Yes
Cut | Paste | Delete | Move | Copy Search	Yes	Delete only
Print	Yes	No
Export Search Query	Yes	No
Run Local Report	Yes	No
Publish to Quest Knowledge Portal	Yes	No
Enable | Disable Alerts	Yes	Alert tab only
Alert History | Delete History	Yes	No
Enable | Disable Report	Yes	Report tab only
Set As My Favorite	Yes	No
Search Properties Tabs	Yes	Yes
Save | Save As | Run Search	Yes	Yes
Info Tab: Search Limit	Yes	Yes
Info Tab: Refresh Interval	Yes	No
Info Tab: Show as Widget	No	Yes
Who Tab: Add | Delete criteria	Yes	Yes
Who Tab: Add Wildcard Expression	Yes: Add button on tab	Yes: Tab on dialog
Who Tab: Add With Events	Yes: Button on tab	Yes: Tab on dialog
Who Tab: Include Event Source Initiator	Yes	Yes
What Tab: Add	Yes	Yes
		NOTE: Registry, Service, Local Account searches are only available using Add With Events.
What Tab: Add With Events	Yes: Button on tab	Yes: Button on dialogs
What Tab: Delete | Edit criteria	Yes	Yes
Where Tab: Add | Delete criteria	Yes	Yes
Where Tab: Add Wildcard Expression	Yes: Add button on tab	Yes: Tab on dialog
Where Tab: Add With Events	Yes: Button on tab	Yes: Tab on dialog
When Tab: Date Interval settings	Yes	Yes
When Tab: Time Interval settings	Yes	Yes
When Tab: Ability to reset settings	Yes	No
Origin Tab: Add | Delete criteria	Yes	Yes
Origin Tab: Add With Events	Yes: Button on tab	Yes: Tab on dialog
Alert Tab: Enable Alert	Yes	Yes
Alert Tab: Enable Smart Alert	Yes	Yes
Alert Tab: History Search Limit	Yes	Yes

Table 52. Change Auditor client comparison

Page/Feature	Available in Windows client?	Available in web client?
Alert Tab: Configure Email	Yes	Yes
Alert Tab: Events per email setting	Yes: Setting on tab	Yes: Setting on dialog
Alert Tab: Time Zone setting	Yes: Setting on tab	Yes: Setting on dialog
Report Tab: Enable reporting	Yes	Yes
Report Tab: Preview report	Yes	Yes
Report Tab: Launch Report Designer	Yes	Yes
Report Tab: Define report schedule	Yes	Yes
Report Tab: Define report configuration	Yes	Yes
Layout Tab: Select columns	Yes	Yes
Layout Tab: Define sort criteria	Yes	Yes
Layout Tab: Define display results format (grid, bar graph or pie chart)	Yes	No
SQL Tab: Copy	Yes	No
XML Tab: Copy	Yes	No
Search Results Page	**Yes**	**Yes**
Data grid view	Yes	Yes
Grid controls to sort, group and filter data	Yes	Yes
Timeline view	No	Yes
Event Details Pane	Yes	Yes
Copy event details	Yes	No
Email event details	Yes	Yes
View knowledge base	Yes	Yes
Add/view comments	Yes	Yes
View user context	Yes	Yes
Run related searches	Yes	Yes
View resource properties	Yes	Yes
Restore value on Active Directory object events	Yes	Yes
Print page	Yes	No
Deployment Page	**Yes**	**No**
Agent Statistics Page	**Yes**	**Yes**
Access by:	View menu command Agent Status Overview hot spot link	Agent Status Overview hot spot link
Start | Stop | Restart agent	Yes	No
Set Agent Uninstalled	Yes	No
Hide | Show Uninstalled agents	Yes	No
View agent logs	Yes	No
Print page	Yes	No
View resource properties	Yes	No

Table 52. Change Auditor client comparison

Page/Feature	Available in Windows client?	Available in web client?
Coordinator Statistics Page	**Yes**	**Yes**
Accessed by:	View menu command Coordinator Status Overview hot spot link	Coordinator Status Overview hot spot link
Set Coordinator Uninstalled	Yes	No
Hide | Show Uninstalled coordinators	Yes	No
Print page	Yes	No
View coordinator logs	Yes	No
Administration Tasks Page	**Yes**	**Yes**
Export/Import setting/templates	Yes	No
Print pages	Yes	No
Configuration Tasks	**Yes**	**Yes**
Agent configuration page	Yes	Yes
Coordinator configuration page	Yes	Yes
Purge Jobs page	Yes	Yes
Report Layouts page	Yes	Yes
Private Alerts and Reports page	Yes	No
Application User Interface page	Yes	Yes
Auditing Tasks	**Yes**	**Yes**
Audit Events page	Yes	Yes
Excluded Accounts page	Yes	Yes
Active Directory Auditing page	Yes	Yes
Active Directory Attribute Auditing page	Yes	Yes
Member of Group Auditing page	Yes	Yes
Excluded AD Query page	Yes	Yes
ADAM (AD LDS) Auditing page	Yes	Yes
ADAM (AD LDS) Attribute Auditing page	Yes	Yes
Exchange Mailbox page	Yes	Yes
Office 365 page	Yes	No
SQL Auditing page	Yes	Yes
SQL Data Level Auditing page	Yes	No
VMware Auditing page	Yes	Yes
SharePoint Auditing page	Yes	Yes
File System Auditing page	Yes	Yes
Registry Auditing page	Yes	Yes
Services Auditing page	Yes	Yes
EMC Auditing page	Yes	Yes
NetApp Auditing page	Yes	Yes
FluidFS Auditing page	Yes	Yes
Web Site Auditing page	Yes	Yes
Protection Tasks	**Yes**	**Yes**

Table 52. Change Auditor client comparison

Page/Feature	Available in Windows client?	Available in web client?
Active Directory Protection page	Yes	Yes
ADAM (AD LDS) Protection page	Yes	Yes
Group Policy Protection page	Yes	Yes
Exchange Mailbox Protection page	Yes	Yes
File System Protection page	Yes	Yes
Shared Overviews Page	**No**	**Yes**
About Change Auditor dialog	**Yes**	**Yes**

About us

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

Our brand, our vision. Together.

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

Contacting Quest

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

Technical support resources

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

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

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