Quest

Quest® Change Auditor 7.6.3

Web Client User Guide

© 2026 Quest Software Inc.

ALL RIGHTS RESERVED.

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

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

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

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

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

Patents

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

Trademarks

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

Legend

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

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

Change Auditor Web Client User Guide
Updated - August 2026
Software Version - 7.6.3

Contents

Install Change Auditor Web Client 5
Introduction 5
Deployment requirements 5
Install web client 6
Troubleshooting tips 7

Web Client Overview 8
Introduction 8
Open the web client 8
Start Page 9
Web client components 9
Heading bar 9
Main web pages 9
Change Auditor settings 10
Customize table content 11
Sort data 11
Resize columns 11
Add or remove columns 11
Expand properties button (right arrow) 12
Filter data 12
Directory object picker 12

Overview Page 15
Introduction 15
Slideshow mode 15
Custom Views mode 16
Overviews/widgets 16
Overview drilldowns page 18

Shared Overviews Administration Page 20
Introduction 20
Manage shared overviews 21

Searches Page 24
Introduction 24
Run searches 25
Create custom searches 25
Search Properties tabs 29
Info tab 29
Who Tab 30
What tab 31
Where tab 43
When tab 45
Origin tab 46

Alert tab 47
Report tab 48
Layout tab 50
SQL tab 51
XML tab 52

Search Results Page 53
Introduction 53
Data grid view 53
Search results grid 54
Event Details pane 54
Timeline view 56
Event markers 56
Navigation Control panel 57
Navigate timeline 58
View event details in Timeline view 59

Change Auditor Client Comparison 60

About us 64
Our brand, our vision. Together. 64
Contacting Quest 64
Technical support resources 64

1

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, and create custom search queries. 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

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.

NOTE: To ensure privacy and data integrity when using the web client Quest requires that you set up SSL on the required IIS Server. See the following documentation for details:

- https://docs.microsoft.com/en-us/iis/manage/configuring-security/how-to-set-up-ssl-on-iis#iis-manager
- https://www.ssl.com/how-to/redirect-http-to-https-with-windows-iis-10/

Install the web client:

1. On the IIS web server, browse to the folder where the Change Auditor package was downloaded, and run the **Quest Change Auditor Web Client (x64).msi** file to open the Change Auditor Web Client Setup wizard.
2. On the Welcome screen, click **Next**.
3. On the Select Installation Folder screen, click **Next** to use the default location. Use **Browse** to specify a different location, then click **Next**.
4. From the Internet Information Services screen, you can select a website for the web client. Only websites with configured HTTPS bindings will be available.
5. 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.

   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.

6. Specify the authentication method to use to make Active Directory requests.
   - Select Simple Authentication and Security Layer (SASL) to use Kerberos or NTLM.
   - Select Secure Socket Layer (SSL) to use certificates.

   IMPORTANT: If you choose SSL, please see the Change Auditor Install Guide for important guidelines.

   NOTE: When making Active Directory requests, credentials and message content are encrypted for both authentication methods.

7. Click **Install**.
8. Click **Finish** to exit the wizard.
9. 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.

- Users who require access to the web client should be added to the ChangeAuditor Operators - <InstallationName> Group. Users added to this group can view Shared Overviews and run searches.
- Users requiring access to the Shared Overviews Administration page in the web client must be added to the ChangeAuditor Administrators - <InstallationName> Group.

  Members of this group can also manage shared searches in the web client.

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

Start the web client:

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

https://<*Web Server Host Name*>/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.

NOTE:

- By default you only have 3 attempts to log on to the web client. Once locked out you will need to wait 15 minutes before you can try to log on again.
- 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.

NOTE: Upgrading the web client

- If version 7.5 (or earlier) Change Auditor web client was previously installed with non-default site or port specification, you may be prompted to uninstall the web client before installing the 7.6 web client.
- After you have upgraded the web client, you may need 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.
- The installer for Change Auditor web client version 7.5 (or earlier) may delete the web site during uninstallation. Ensure you back up your IIS configuration before proceeding with the upgrade. For detailed instructions on managing IIS backups with AppCmd utility, refer to the Microsoft article on Managing IIS backups with Microsoft AppCmd.exe utility.
- Ensure the target IIS web site is configured with HTTPS bindings.

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>"/>`

  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.

2

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 view Change Auditor data using a web browser rather than the Windows client.

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.

   https://<*Web Server Host Name*>/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.

   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.

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.

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.

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.

   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**.

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:
>
> - Active Directory, AD Query, ADAM (AD LDS), Exchange, and Group Policy searches.

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.

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.

3

Overview Page

- Introduction
- Slideshow mode
- Custom Views mode
- Overviews/widgets
- Overview drilldowns 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.

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

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.

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.

4

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.

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.

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.

   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.

> **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.

> **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:

> **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.

5

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 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.

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.

> **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 ▪ **Microsoft Entra -** Add Microsoft Entra dialog. ▪ **AD Query** - Add Active Directory Container dialog ▪ **ADAM (AD LDS)** - Add ADAM (AD LDS) Container dialog ▪ **Exchange** - Add Exchange Container dialog ▪ **Microsoft 365 Exchange Online** - Microsoft 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 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.

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.

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.

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. 4 Click **Add** to add criteria to the selection list. 5 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.

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.

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
Microsoft Entra **NOTE:** When Microsoft Entra 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 Microsoft Entra ID. **Add Microsoft Entra 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 Microsoft Entra admin center”. 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 Microsoft Entra ID changes. **NOTE:** Use **Add With Events** to select from a list of Microsoft Entra ID changes that already have an event associated with it in the database. **NOTE:** Use **Add all events** to add all Microsoft Entra 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
Microsoft 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' Microsoft 365 Exchange Online events: **All Microsoft 365 Exchange Online Events**, **All Microsoft 365 Exchange Online Mailbox Events**, or **All Microsoft 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. **Microsoft 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: Change Auditor for Windows File Systems Change Auditor for NetApp Change Auditor for EMC	Select to search for specific file system events. **Add File System Path dialog**: 1 Enter a file or folder path. 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 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.

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.

Table 12. Add Agents, Domains, Sites dialog

Tab	How to add criteria
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.

NOTE: When this check box is checked, the **Date Interval/Time Interval** settings will be deactivated.

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.

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 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, through email, SNMP, or WMI.

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.

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).
- **Email**: Select to dispatch 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.

  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.

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.

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.

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 in the Windows client.

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

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.

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.

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.

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.

6

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.

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.

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.
Coordinator ID	The coordinator that processed the event.

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.

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.

  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.)

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.

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.

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.

7

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 18. 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 18. 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
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
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
Alert Tab: Configure Email	Yes	Yes
Alert Tab: Events per email setting	Yes: Setting on tab	Yes: Setting on dialog

Table 18. Change Auditor client comparison

Page/Feature	Available in Windows client?	Available in web client?
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: 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
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

Table 18. Change Auditor client comparison

Page/Feature	Available in Windows client?	Available in web client?
Print page	Yes	No
View coordinator logs	Yes	No
Administration Tasks Page	**Yes**	**No**
Export/Import setting/templates	Yes	No
Print pages	Yes	No
Configuration Tasks	**Yes**	**No**
Agent configuration page	Yes	No
Coordinator configuration page	Yes	No
Purge Jobs page	Yes	No
Report Layouts page	Yes	No
Private Alerts and Reports page	Yes	No
Application User Interface page	Yes	No
Auditing Tasks	**Yes**	**No**
Audit Events page	Yes	No
Excluded Accounts page	Yes	No
Active Directory Auditing page	Yes	No
Active Directory Attribute Auditing page	Yes	No
Member of Group Auditing page	Yes	No
Excluded AD Query page	Yes	No
ADAM (AD LDS) Auditing page	Yes	No
ADAM (AD LDS) Attribute Auditing page	Yes	No
Exchange Mailbox page	Yes	No
Microsoft 365 page	Yes	No
SQL Auditing page	Yes	No
SQL Data Level Auditing page	Yes	No
SharePoint Auditing page	Yes	No
File System Auditing page	Yes	No
Registry Auditing page	Yes	No
Services Auditing page	Yes	No
EMC Auditing page	Yes	No
NetApp Auditing page	Yes	No
Web Site Auditing page	Yes	No
Protection Tasks	**Yes**	**No**
Active Directory Protection page	Yes	No
ADAM (AD LDS) Protection page	Yes	No
Group Policy Protection page	Yes	No
Exchange Mailbox Protection page	Yes	No
File System Protection page	Yes	No
Shared Overviews Page	**No**	**Yes**
About Change Auditor dialog	**Yes**	**Yes**

About us

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

Our brand, our vision. Together.

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

Contacting Quest

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

Technical support resources

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

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

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