Quest

Quest® Change Auditor for SQL Server® 7.6

User Guide

© 2025 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.
20 Enterprise, Suite 100
Aliso Viejo, CA 92656

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

Patents

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

Trademarks

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

Legend

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

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

Change Auditor for SQL Server User Guide
Updated - July 2025
Software Version - 7.6

Contents

Change Auditor for SQL Server Overview 4
Introduction 4
Deployment requirements 4
Client components/features 5

Getting Started 8
Introduction 8
Apply SQL Server auditing template 9
Make changes to the default SQL instance and run a report 9

SQL Server Auditing 11
Introduction 11
SQL Auditing page 11
SQL Auditing templates 12
SQL Auditing wizard 16
SQL Server event logging 18

SQL Data Level Auditing 19
Introduction 19
SQL Data Level Auditing page 19
SQL Data Level Auditing templates 20
SQL Data Level Auditing wizard 22

SQL Extended Events Auditing (Preview) 25
Introduction 25
SQL Extended Events Auditing templates 25

SQL Searches/Reports 26
Introduction 26
Create custom SQL searches 26
Create custom SQL Data Level searches 28
Create custom SQL Extended Events searches (Preview) 29

Disabled SQL Events 30

About us 33
Our brand, our vision. Together. 33
Contacting Quest 33
Technical support resources 33

1

Change Auditor for SQL Server Overview

- Introduction
- Deployment requirements
- Client components/features

Introduction

Change Auditor for SQL Server provides database auditing to secure SQL database assets with extensive, customizable auditing and reporting for all critical SQL Server changes including broker, database, object, performance, transaction events, changes to databases and tables, plus errors and warnings. SQL auditing helps tighten enterprise-wide change and control policies by tracking user and administrator activity such as database additions and deletions, granting and removing SQL access, and so on.

To enable SQL Server auditing, you must assign templates to the Change Auditor agents which define the SQL instances and event classes to audit; SQL Data Level auditing is assigned to a single agent when a template is created.

To enable SQL Extended Events auditing (preview feature), you must define a SQL Extended Events auditing template for each target SQL Server instance to be audited by Change Auditor.

This guide has been prepared to assist you in becoming familiar with Change Auditor for SQL Server. It is intended for network administrators, consultants, analysts, and any other IT professionals using the product.

- For information on the core functionality available in Change Auditor regardless of the product license that has been applied, see the Change Auditor User Guide and the Change Auditor Installation Guide.
- For event details, see the Change Auditor for SQL Server Event Reference Guide.

Deployment requirements

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

Client components/features

The following table lists the client components and features that require a valid Change Auditor for SQL Server license.

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

Table 1. Change Auditor for SQL Server client components/features

Client page	Feature
Administration Tasks tab	Agent Configuration page • Event Logging - enable/disable SQL Server event logging Audit Task list: • SQL Server **NOTE:** See SQL Server Auditing, and SQL Data Level Auditing for information about creating templates.
Events	Facilities: • Admin Extended Events • Analytic Extended Events • Operational Extended Events • SQL Broker Event • SQL CLR Event • SQL Cursors Event • SQL Database Event • SQL Data Level • SQL Deprecation Event • SQL Errors and Warnings Event • SQL Full Text Event • SQL Locks Event • SQL Objects Event • SQL OLEDB Event • SQL Performance Event • SQL Progress Report Event • SQL Query Notifications Event • SQL Scan Event • SQL Security Audit Event • SQL Server Event • SQL Session Event • SQL Stored Procedures Event • SQL Transactions Event • SQL TSQL Event • SQL User-Configurable Event
Search Properties	What tab • Subsystem | SQL **NOTE:** See SQL Searches/Reports for information about using the What tab to create custom SQL search queries.
Searches page	Built-in reports: • All reports that include the events in the facilities listed above.

Table 1. Change Auditor for SQL Server client components/features

Client page	Feature
Advanced tab/Search Results page **NOTE:** The data gathered will be dependent on whether you are auditing SQL, SQL Data Level Auditing, or SQL Extended Events.	Columns: • SQL Application Name • SQL Category • SQL Changed Columns • SQL Client Process ID • SQL Database ID • SQL Database Name • SQL Event Class • SQL Event Name • SQL Event SubClass • SQL Host Name • SQL Instance Name • SQL IsSystem • SQL Linked Server Name • SQL Object ID • SQL Object ID2 • SQL Object Name • SQL Object Type • SQL Owner ID • SQL Owner Name • SQL Package Name • SQL Parent Name • SQL Provider Name • SQL Row Counts • SQL Session Login Name • SQL SPID • SQL Success • SQL Table Name • SQL Text Data • SQL Transaction ID

Table 1. Change Auditor for SQL Server client components/features

Client page	Feature
Alert Body Configuration dialog - Event Details tab	Variables (email tags): • SQL_APPLICATIONNAME • SQL_CLIENTPROCESSID • SQL_DATABASEID • SQL_DATABASENAME • SQL_EVENTCLASS • SQL_EVENTSUBCLASS • SQL_HOSTNAME • SQL_INSTANCENAME • SQL_ISSYSTEM • SQL_LINKEDSERVERNAME • SQL_OBJECTID • SQL_OBJECTID2 • SQL_OBJECTNAME • SQL_OBJECTTYPE • SQL_OWNERID • SQL_OWNERNAME • SQL_PARENTNAME • SQL_PROVIDERNAME • SQL_ROWCOUNTS • SQL_SESSIONLOGINNAME • SQL_SPID • SQL_SUCCESS • TEXTDATA **NOTE:** See the Change Auditor User Guide for a description of these email tags and how to configure alert email notifications.

2

Getting Started

- Introduction
- Apply SQL Server auditing template
- Make changes to the default SQL instance and run a report

Introduction

To capture event data for SQL, SQL Data Level, and SQL Extended Events, ensure that your system meets the minimum requirements. For details, see Deployment requirements.

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

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

Auditing SQL Server events

To capture SQL events in Change Auditor, you must define the SQL instances to be audited and the events to be captured:

1. Assign the pre-defined 'Best Practice SQL Auditing Template', that audits key SQL events that occur on the default SQL instance, to an agent configuration.

   Or create a new SQL Auditing template which specifies the SQL instances and events to audited and assign this template to an agent configuration.

2. Assign the agent configuration to agents.

Auditing SQL Data Level events

To capture SQL Data Level events, you must assign SQL Data Level auditing templates to an agent when you create the template. Each audited database requires one template assigned to a single agent.

For information on creating templates, see To create a new SQL Data Level auditing template:.

Auditing SQL Extended Events

To capture SQL Extended Events data, you must create an SQL Extended Events auditing template. A remote agent may be specified, otherwise an agent must be installed on the SQL Server host to be audited.

For information on creating templates, see the Change Auditor PowerShell Command Guide.

Apply SQL Server auditing template

Change Auditor for SQL Server includes a configured auditing template, named Best Practice SQL Auditing Template that you can apply to an agent configuration to audit the default SQL instance to capture key SQL events or used as a starting point for creating a new template.

The following steps walk you through the process of applying the pre-defined SQL Auditing template to get you started.

To assign the Best Practices SQL Auditing template to an agent configuration:

1. Open the Administration Tasks tab.
2. Click **Configuration**.
3. Select **Agent** (in the Configuration task list) to open the Agent Configuration page.
4. Click **Configurations**.

   This displays the Configuration Setup dialog, which contains a list of configuration definitions available.

   > **NOTE:** The Default Configuration is the only configuration listed if you have not defined any other agent configurations. For more information about defining agent configurations, see the Change Auditor User Guide.

5. On the Configuration Setup dialog, use one of the following methods to assign this template to an agent configuration:
   - Select the Best Practices SQL Auditing template and drag it onto a configuration in the Configuration list.
   - Select a configuration from the Configuration list and drag it onto the Best Practices SQL Auditing template.
   - Select a configuration, then select the Best Practices SQL Auditing template, right-click and select **Assign**.
   - Select a configuration, then select the Best Practices SQL Auditing template, click in the corresponding **Assigned** cell and click **Yes**.
6. Click **OK** to close the Configuration Setup dialog and return to the Agent Configuration page.
7. Select an agent from the list, click **Assign** and then select the agent configuration to assign to the agent from the displayed dialog. Click **OK** to save your selection and close the Agent Assignment dialog.
8. On the Agents Configuration page, select the agents assigned to use the modified agent configuration (**Auditing** appears in the **SQL** column) and click **Refresh Configuration** to ensure the agents are using the latest configuration.

   > **NOTE:** If you do not refresh the agent's configuration, the agent will automatically check for a new agent configuration based on the polling interval setting (located on the System Settings tab of the Configuration Setup dialog). The default is every 15 minutes.

Make changes to the default SQL instance and run a report

1. To test SQL Server auditing, make some changes to the default SQL instance.

   For example:
   - add a database user

- add a database role
- grant or revoke database access to a database user
- delete the database user added above
- delete the database role added above

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

3 Open the Searches tab.

4 Expand the **Shared | Built-in | Recommended Best Practice | SQL Server** folder in the left pane.

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

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

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

3

SQL Server Auditing

- Introduction
- SQL Auditing page
- SQL Auditing templates
- SQL Auditing wizard
- SQL Server event logging

Introduction

The SQL Auditing page on the Administration Tasks tab displays details about each SQL Auditing template created and allows you to add new auditing templates or modify and delete templates. It will initially contain an entry for the Best Practice SQL Auditing Template that ships with Change Auditor.

NOTE: Due to a Microsoft hotfix, Change Auditor agents will not capture SQL-related events until the following action is taken on each SQL Server to be monitored:

1. Select **Start | All Programs | Microsoft SQL Server | Configuration Tools | SQL Server Configuration Manager**.
2. Select the **SQL Server Services** node.
3. Right-click **SQL Server (MSSQLSERVER)** and select **Properties.**
4. Select the **Startup Parameters** tab.
5. Enter **-T1906** and click **Add**.
6. Restart the **SQL Server (MSSQLSERVER)** service.

   Repeat steps 3 through 6 for each instance on the server (SQL Server (instance name)).

NOTE: Launching SQL Server Configuration Manager with UAC enabled can cause issues with SQL server properly writing to C:\Program Files\Microsoft SQL Server\MSSQL13.MSSQLSERVER\MSSQL\Binn\etwcnf.xml after the trace flag is enabled.
Once you add the - T1906 flag, ensure the etwcnf.xml exists and is not empty.

NOTE: The folder path changes based on the version of SQL.

This section provides instructions for creating SQL Auditing templates, as well as a description of the Best Practice SQL Auditing template, SQL Auditing page and SQL Auditing wizard. For a description of the dialogs mentioned, see the online help. For more information about agent configurations, refer to the Change Auditor User Guide.

SQL Auditing page

The SQL Auditing page is displayed when **SQL Server** is selected from the Auditing task list in the navigation pane of the Administration Tasks tab. From this page you can start the SQL Auditing wizard to specify the SQL instances and the operations to audit. You can also edit existing templates and remove templates that are no longer being used.

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

The SQL Auditing page contains an expandable view of all the SQL Auditing templates that have been defined. Initially, only the Best Practice SQL Auditing template will be listed on this page. To add a new template to this list, click the **Add** tool bar button. Once added, the following information is provided for each template:

Template

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

Status

Indicates whether the auditing template is enabled or disabled.

Instance

This field is used for filtering data.

Operations

Displays the events selected for auditing on the Events tab of the wizard. Hover your mouse over this cell to view all of the events included in the template.

Filters

Displays the column filters applied to a template.

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

Instance

Displays the name of the SQL instance selected on the first page of the wizard.

Status

Indicates whether auditing for the selected instance is enabled or disabled.

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

SQL Auditing templates

To enable SQL Server auditing, you must add a SQL Auditing template to an agent configuration, which can then be assigned to the appropriate agents. Change Auditor for SQL Server ships with a pre-defined template that you can use to audit key events on the default SQL server instance or you can create a template to specify the SQL instances and SQL Server operations to audit.

Best Practice SQL Auditing template

The Best Practice SQL Auditing template is a pre-defined template that audits the default SQL instance for the following SQL Server operations:

- Audit Add DB User

- Audit Add Login
- Audit Add Login to Server Role
- Audit Add Member to DB Role
- Audit Add Role
- Audit Change Database Owner
- Audit Change Member in DB Role
- Audit Create Database
- Audit Drop Database
- Audit Drop DB User
- Audit Drop Login from Server Role
- Audit Drop Member from DB Role
- Audit Drop Role
- Audit Grant Database Access to DB User
- Audit Revoke Database Access from DB User
- Data File Auto Grow
- Data File Auto Shrink
- Log File Auto Grow
- Log File Auto Shrink

You can assign this template to an agent configuration or can use it as a base for creating your own SQL auditing templates.

For instruction on how to assign the default Best Practices SQL Auditing template to an agent configuration, see Getting Started.

To create a new SQL server auditing template:

NOTE: You can use the Best Practice SQL Auditing Template as a starting point for creating a template. That is, you can edit this pre-defined template to add additional SQL server operations or define column filters. You can also, add a new instance to the auditing list and copy the pre-defined operations and filters to the new instance. See the To modify a template: procedure for more information.

1. Open the Administration Tasks tab.
2. Click **Auditing**.
3. Select **SQL Server** (under the Applications heading in the Auditing task list) to open the SQL auditing page.
4. Click **Add** to start a wizard which steps you through the process of creating a SQL auditing template.
5. Enter a name for the template and select the SQL instance to audit.
   - Select the **Default** option to audit the default instance. Select **Add** to add it to the SQL Instance list.
   - Select the **Named** option to audit a named instance. Select the browse button, select a SQL instance from the list displayed and click **OK** to close the dialog. Click **Add** to add the SQL instance to the auditing list.
   - Select **All Instances** to audit all the SQL instances on the server. Click **Add** to add it to the SQL Instance list.
6. On the second page of the wizard, select the operations (facilities or event classes) to audit. You must select at least one event.

   Select an entry from the list box at the top of the page, expand the **Add** button and click one of the following commands:

- Use the **Add | Add This Event** button to add individual events.
- Use the **Add | Add All Events in Facility** option to add all events in the selected facility.

7 On the third page of the wizard, optionally define column filters to capture only a subset of transactions.

- Select/highlight an entry from the data grid.
- In the **Filter where** fields, enter the operator and value to use in the filter. In the first field (left) use the drop-down menu to select the operator (e.g., Like or Not Like; =, !=, <= or >=). The operators listed are based on the entry selected in the **Filters** list above. In the second field (right) enter the value or string to use in the filter.

  NOTE: You an use the following wildcard characters in LIKE expressions for non-exact string matches:
  - Use an asterisk (*) to match zero or more characters.
  - Use a percent sign (%) to match zero or more characters.
  - Use an underscore (_) to match a single character.

- Click **Add** to add it to the Filter list.

  NOTE: To add multiple filters, select the column filter row after which the new filter is to be added, and then use the **Filter where** fields to specify the new criteria. By default, when multiple filters are specified these filters are 'ANDed' together and all filters must be met in order to be considered a match. To use the 'OR' operator instead, click in the left-most column of a column filter row and select OR from the drop-down. When filters are 'ORed' together, then only one of the filters must be met in order to be considered a match.

  When both 'AND' and 'OR' operators are present in the filter list, 'ORed' filters are evaluated first and their results are used by the 'AND' filter.

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

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

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

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

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

- On the Agent Configuration page, select one or more agents from the agent list and click **Assign**.
- On the Agent Assignment dialog, select the configuration definition to assign to the selected agents and click **OK**.
- On the Agent Configuration page, select the agents assigned to use the modified agent configuration and click **Refresh Configuration** to ensure the agents are using the latest configuration.

NOTE: If you do not refresh the agent's configuration, the agent automatically checks for a new agent configuration based on the polling interval setting (located on the System Settings tab of the Configuration Setup dialog). The default is every 15 minutes.

IMPORTANT: When multiple SQL auditing templates are assigned to an agent configuration, the criteria specified in the last template assigned to the agent takes precedence.

To modify a template:

1 On the SQL auditing page, select the template to be modified and click **Edit**.

2 This opens the SQL Auditing wizard, where you can modify the SQL instance, events and/or filters included in the template. For example:

- On the first page of wizard, you can change the name of the template or add a new SQL instance to the selected auditing template.

  NOTE: If you add a new instance to the SQL instance list and want to use the same operations and filters that were previously defined for a SQL instance that is already in the list, simply click on the 'old' SQL instance and drag it onto the 'new' entry.

- On the second page of the wizard, you can add or remove SQL events from the selected auditing template.
- On the third page of the wizard, you can add, modify or remove column filters from the selected auditing template.

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

To disable an auditing template:

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

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

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

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

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

To disable the auditing of a SQL instance in a template:

1 On the SQL auditing page, use one of the following methods to disable a SQL instance in an auditing template:

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

The entry in the **Status** column for the selected SQL instance will change to 'Disabled'.

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

To delete an auditing template:

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

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

To delete a SQL instance from a template:

1 On the SQL auditing, select the SQL instance to be deleted and click **Delete | Delete SQL Instance**.

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

NOTE: If the SQL instance is the last one in the template, deleting this SQL instance also deletes the template.

SQL Auditing wizard

The SQL Auditing wizard is displayed when you click **Add** or **Edit** on the SQL Auditing page. This wizard steps you through the process of creating a new template, identifying the SQL instances to be included in the template. You will also use this wizard to modify a previously defined template.

NOTE: A red flashing icon indicates that you have not yet entered the required information. Hovering your cursor over this icon displays a tool tip explaining what needs to be entered.

Table 2. SQL Auditing wizard fields and controls

Create or modify a SQL Auditing Template page	
On the first page of the wizard, enter a name for the template and select the SQL instance to audit.	
Template Name	Enter a descriptive name for the template being created.
Audit SQL Instance	Select one of the following options: • **Default** - This option is selected by default and will use the default SQL instance (MSSQLSERVER) found on an agent that is using the SQL Server Auditing template. • **Named** - Select this option to use a named instance instead of the default SQL instance. When this option is selected, the name field will be activated allowing you to enter a SQL named instance. Or use the browse button to the right of this field to select from a list of available servers. Selecting the browse button opens the Select a SQL Instance dialog which displays a list of available servers. • **All Instances** - Select this option to audit all SQL instances on a SQL server.
Add	Use to move the entry in the Audit SQL Instance text box to the selection list. **NOTE:** Even if you select the Default SQL instance or All Instances, you must click **Add** to include it in the SQL Instance list.
Remove	Select an entry in the selection list and click **Remove** to remove it from the template.
SQL Instance list	The list box, located across the bottom of this page, displays the SQL instances selected for auditing. **NOTE:** If you add a new named instance to the SQL instance list and want to use the same operations and filters that were previously defined for a SQL instance that is already in the list, simply click on the 'old' SQL instance and drag it onto the 'new' entry.
Select the changes in the SQL instance(s) to audit page	
From this page, select the SQL Server operations (event classes) to audit on the selected SQL instance. You must select at least one operation.	
Event Classes	The data grid across the top of the page displays all the SQL event classes available for auditing. Select/highlight an event class and use the appropriate add option to add either the individual event class or all events in the selected facility. This grid displays the following information for each event class: • **Facility** - the facility to which each event class belongs • **Event Class** - the events available for auditing • **Severity** - the current severity level assigned to each event • **Status** - indicates whether the event is currently enabled or disabled
Add | Add This Event	Use to add the selected event class to the Audit list box at the bottom of the page.

Table 2. SQL Auditing wizard fields and controls

Add | Add All Events in Facility	Use to add all event classes in the selected facility to the Audit list box at the bottom of the page.
Remove	Use to remove the selected entry from the Audit list box.
Selection list	This list box displays the facilities and/or event classes to be included in the selected auditing template.
(Optional) Select column filters page	
Using the Select Column Filters page you can optionally define column filters to limit the data retrieved. These filters allow you to capture only the required information in high traffic databases.	
Filters	The data grid across the top of the page displays the SQL columns available for filtering. Select/highlight an entry and then use the **Filter where** fields to define the operator and values to be used in the filter.
Filter where ...	In the first field (left) use the drop-down menu to select the operator (e.g., Like or Not Like; =, !=, <= or >=). The operators listed are based on the entry selected in the Filters list above. In the second field (right) enter the value or string to be used in the filter. **NOTE:** Valid wildcard characters that can be used in LIKE expressions for non-exact string matches include: • Asterisk (*) to match zero or more characters • Percent sign (%) to match zero or more characters • Underscore (_) to match a single character For example, to limit the data retrieval to all databases that begin with 'Change' (e.g., Change Auditor, ChangeAuditor_Archive_2011, ChangeManager, etc.) • Select **DatabaseName** from the Filters list. • Select **LIKE** in the first field. • Enter **Change%** in the second field. • Click **Add** to add it to the list. **NOTE:** To add multiple filters, select the column filter row after which the new filter is to be added, and then use the **Filter where** fields to specify the new criteria. By default, when multiple filters are specified these filters are 'ANDed' together and all filters must be met in order to be considered a match. To use the 'OR' operator instead, click in the left-most column of a column filter row and select OR from the drop-down. When filters are 'ORed' together, then only one of the filters must be met in order to be considered a match. **NOTE:** When both 'AND' and 'OR' operators are present in the filter list, 'ORed' filters are evaluated first and their results are used by the 'AND' filter.
Add	Use to move the filter entered above to the Column Filter list at the bottom of the page.
Remove	Use to remove the selected entry from the Column Filter list.
Modify	Use to change the operator or value of the filter selected in the Column Filter list.
Column Filter list	This list box displays the column filters defined for this SQL Auditing template.

SQL Server event logging

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

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

To enable SQL Server event logging:

1. Open the Administration Tasks tab and click **Configuration**.
2. Select **Agent**.
3. Click **Event Logging** and select **SQL**.
4. Click **OK** to save your selection and close the dialog.

4

SQL Data Level Auditing

- Introduction
- SQL Data Level Auditing page
- SQL Data Level Auditing templates
- SQL Data Level Auditing wizard

Introduction

SQL Data Level auditing allows you to audit changes to databases and tables. Separate SQL Data Level auditing templates must be defined for each target database to be audited by Change Auditor.

The SQL Data Level Auditing page on the Administration Tasks tab displays details about each SQL Data level auditing template created and allows you to add, modify, and delete templates.

This section provides instructions for creating SQL Data Level auditing templates, as well as a description of the SQL Data Level auditing page and SQL Data Level Auditing wizard. For a description of the dialogs mentioned, see the online help. For more information about agent configurations, refer to the Change Auditor User Guide.

Ensure that you have reviewed the requirements that must be in place for SQL Data Level auditing. For more information, see Client components/features.

SQL Data Level Auditing page

The SQL Data Level Auditing page is displayed when **SQL Data Level** is selected from the Auditing task list in the navigation pane of the Administration Tasks tab. From this page you can launch the SQL Data Level Auditing wizard to specify the SQL instances and the operations to audit. You can also edit existing templates and remove templates that are no longer being used.

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

The SQL Data Level Auditing page contains an expandable view of all the SQL Data Level Auditing templates that have been defined. To add a new template, click the **Add** tool bar button. Once added, the following information is provided for each template:

Template

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

Status

Indicates whether the auditing template is enabled or disabled.

Database

Displays the target database.

Operations

Displays the events selected for auditing on the Events tab of the wizard. Hover your mouse over this cell to view all of the events included in the template.

Filters

Displays the column filters applied to a template.

Sensitive Columns

Displays the columns that have been selected in the Sensitive column data option in the template wizard. Due to the nature of this data, it will display as “***” in Event Details pane and no actual values will be stored in the database.

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

SQL Data Level Auditing templates

To enable SQL Data Level auditing in Change Auditor, you must create a SQL Data Level auditing template which specifies the SQL server, Instance, and the database to audit. Change Auditor agents must be installed on SQL servers/SQL cluster nodes before configuring their templates.

NOTE: For SQL clusters a template must be configured for each database/node combination. For example, a single database in a two node cluster would require two templates. One for Node1 and another for Node2.

NOTE: When multiple enabled SQL Data Level templates are auditing the same database, each template is analyzed separately and an event only needs to match one template to enter the event in the Change Auditor database, even if a second template specifically excludes it with, for example, a NOTLIKE filter. Sensitive column configuration values from the enabled templates are then merged and applied to incoming events.

For example:

- Template1 is enabled and configured with sensitive columns PERSON.NAME, PERSON.PAYGRADE.
- Template2 is enabled and configured with sensitive column PERSON.ADDRESS.
- Template3 is disabled and configured with sensitive column PERSON.DEPARTMENT.

For a new event, data in the PERSON.NAME, PERSON.PAYGRADE and PERSON.ADDRESS fields will display as "***".

To create a new SQL Data Level auditing template:

1. Open the Administration Tasks tab.
2. Click **Auditing**.
3. Select **SQL Data level** (under the Applications heading in the Auditing task list) to open the SQL Data Level Auditing page.
4. Click **Add** to open the SQL Data Level auditing wizard which will step you through the process of creating a template.

5 Enter a name for the template and select the SQL instance to be audited.

- Select the SQL server to be audited.
- Select the **Default** option to audit the default instance.
- Select the **Named** option to audit a named instance.
- Select the target database to be audited.

  The logged in account is used to attempt to populate the available databases and their data. If the logged in account does not have the proper access rights, SQL Server authentication credentials are required.
- Select the agent server to perform the auditing. If a SQL Server cluster is specified in the Server field, you can pick the agent/node by clicking the browse button.
- Enter the credentials required for the agent to access the SQL sever. Click **Test credentials** to ensure the specified database can be opened on the target server.

  NOTE: If the target SQL Server's domain does not trust the Change Auditor client's domain, the test for Windows Authentication may fail even though the agent credentials are valid.

6 On the second page of the wizard, select the operations (event classes) that are to be audited. At least one event must be selected.

Select an entry from the list box at the top of the page, and select **Add** to add individual events.

7 On the third page of the wizard, optionally define column filters to capture only a subset of transactions.

- Select/highlight an entry from the data grid.
- In the **Filter where** fields, enter the operator and value to be used in the filter. In the first field (left) use the drop-down menu to select the operator (In, Not in, Like or Not Like; =, !=). The operators listed are based on the entry selected in the **Filters** list above. In the second field (right) enter the value or string to be used in the filter.

  NOTE: The following wildcard characters can be used in LIKE expressions for non-exact string matches:
  - Use a percent sign (%) to match zero or more characters.
  - Use an underscore (_) to match a single character.

  NOTE: Commas (,) can be used to separate individual values when the 'in' and 'not in' operators are is selected.

  NOTE: When setting filters, if there is need to remove multiple objects of the same "type" (for example, TableName) using the != (not equal to) operator, only use the "AND" joiner for the different lines. If "OR" is used in the case, the resulting filter statement will always evaluate to TRUE, and forward the event.

- Click **Add** to add it to the Filter list at the bottom of the page.

  NOTE: To add multiple filters, select the column filter row after which the new filter is to be added, and then specify whether all criteria must be met or only some of the criteria.

  If **Join filters with AND** is selected, all filters specified must be satisfied before an event can be audited. If **Join filters with OR** is selected, only one of the specified filters needs to be satisfied.

8 On the next page of the wizard, you can specify the columns within a table that are deemed to potentially include sensitive information. Select **Refresh Columns** to update the data. Once these columns are identified, their data will not be recorded in the database and will display in the Event Details pane as "***" to maintain privacy.

9 Clicking **Finish** creates the template, close the wizard, and return to the SQL DL Auditing page, where the newly created template will now be listed.

10 Select the Change Auditor agent from the Configuration page and click **Refresh Configuration**.

NOTE: If you do not refresh the agent's configuration, the agent will automatically check for a new agent configuration based on the polling interval setting (located on the System Settings tab of the Configuration Setup dialog). The default is every 15 minutes.

To modify a template:

1. On the SQL Data Level Auditing page, select the template to be modified and click **Edit**.
2. This will display the Data Level Auditing wizard, where you can modify the SQL server, instance, database, assigned agent, events and/or filters included in the template. For example:
   - On the first page of wizard, you can change the name of the template, change the SQL server, instance, or database.
   - On the second page of the wizard, you can add or remove SQL events from the selected auditing template.
   - On the third page of the wizard, you can add, modify or remove column filters from the selected auditing template.
   - On the fourth page of the wizard, you can add, modify, or remove the sensitive columns.
3. Click **Finish** to save the changes.

To disable an auditing template:

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

1. On the SQL Data Level Auditing page, use one of the following methods to disable an auditing template:
   - Place your cursor in the **Status** cell for the template to be disabled, click the arrow control and select **Disabled**.
   - Right-click the template to be disabled and select **Disable**.

   The entry in the **Status** column for the template will change to 'Disabled'.
2. To re-enable the auditing template, use the **Enable** option in either the **Status** cell or right-click menu.

To delete an auditing template:

1. On the SQL Data Level Auditing page, select the template to be deleted and click **Delete | Delete Template**.
2. A dialog will be displayed confirming that you want to delete the selected template. Click **Yes**.

SQL Data Level Auditing wizard

The SQL Data Level Auditing wizard opens when you click **Add** or **Edit** on the SQL Data Level Auditing page. This wizard steps you through the process of creating a template, identifying the SQL server, instances, and database to included in the template. You can also use this wizard to modify a previously defined template.

The following table provides a description of the fields and controls in the SQL DL auditing wizard.

NOTE: A red flashing icon indicates that you have not yet entered the required information. Hovering your cursor over this icon displays a tool tip explaining what needs to be entered.

Table 3. SQL Auditing wizard

Create or modify a SQL Data Level Auditing Template page: On the first page of the wizard, enter a name for the template and select the SQL instance to audit.	
Template Name	Enter a descriptive name for the template being created.
Server	Select the SQL server to audit. If the server is a cluster, select the cluster name, not an individual node.
SQL Instance	Select one of the following options: • **Default** - This option is selected by default and will use the default SQL instance (MSSQLSERVER) found on an agent that is using the SQL Server Auditing template. • **Named** - Select this option to use a named instance instead of the default SQL instance. When this option is selected, the name field will be activated allowing you to enter a SQL named instance.
Database	Select the target database to audit. The logged in account is used to attempt to populate the available databases and their data.If the logged in account does not have the proper access rights, SQL Server authentication credentials are required.
Agent Server	Select the agent server to perform the auditing. **NOTE:** If a SQL Server cluster is specified in the Server field, you can pick the agent/node by clicking the browse button.
Agent Credentials	Enter the credentials required for the agent to access the SQL sever. Click **Test Credentials** to ensure the specified database can be opened on the target server. **NOTE:** If the target SQL Server's domain does not trust the Change Auditor client's domain, the test for Windows Authentication may fail even though the agent credentials are valid.
Select the operations to audit page: From this page, select the SQL Data Level operations (event classes) to audit on the selected SQL instance. You must select at least one operation.	
Event Classes	The data grid across the top of the page displays all of the SQL event classes available for auditing. Select/highlight an event class and use the appropriate add option to add either the individual event class or all events in the selected facility. This grid displays the following information for each event class: • **Event Class** - the events available for auditing • **Severity** - the current severity level assigned to each event • **Status** - indicates whether the event is currently enabled or disabled
Add event	Select the operations (event classes) that are to be audited. At least one event must be selected.
Remove	Use to remove the selected entry from the Audit list box.
Select auditing filters page: Using the filtering page you can optionally define criteria to limit the data retrieved. These filters allow you to capture only the required information in high traffic databases.	
Filters	The data grid across the top of the page displays the SQL columns available for filtering. Select/highlight an entry and then use the **Filter where** fields to define the operator and values to be used in the filter.

Table 3. SQL Auditing wizard

Filter where	In the first field (left) use the drop-down menu to select the operator (In, Not in, Like or Not Like; =, !=). The operators listed are based on the entry selected in the **Filters** list above. In the second field (right) enter the value or string to be used in the filter In the second field (right) enter the value or string to be used in the filter. **NOTE:** The following wildcard characters can be used in LIKE expressions for non-exact string matches: • Use a percent sign (%) to match zero or more characters. • Use an underscore (_) to match a single character. **NOTE:** Commas (,) can be used to separate individual values when the 'in' and 'not in' operators are is selected. **NOTE:** To add multiple filters, select the column filter row after which the new filter is to be added, and then specify whether all criteria must be met or only some of the criteria. **NOTE:** When setting filters, if there is need to remove multiple objects of the same "type" (for example, TableName) using the != (not equal to) operator, only use the "AND" joiner for the different lines. If "OR" is used in the case, the resulting filter statement will always evaluate to TRUE, and forward the event. If 'and' is selected, all filters specified must be satisfied before an event can be audited. If 'or' is selected, only one of the specified filter needs to be satisfied.
Add	Use to move the filter entered above to the Column Filter list at the bottom of the page.
Remove	Use to remove the selected entry from the Column Filter list.
Modify	Use to change the operator or value of the filter selected in the Column Filter list.
Specify columns with sensitive data page: From here you can specify the columns within a table that are deemed to potentially include sensitive information.	
Add\Remove	The data grid across the top of the page displays the SQL table/columns/ and data type. Select/highlight an entry and then use the Add and Remove buttons to define the values to be used in the filter. Select **Refresh Columns** to update the data. Once these columns are identified, they will not record values in the database and will display as "***" in the Event Details pane to maintain privacy. **NOTE:** When multiple SQL Data Level templates are auditing the same database, all sensitive column configurations defined in any of the enabled templates is applied. For example: • Template1 is enabled and configured with sensitive columns PERSON.NAME, PERSON.PAYGRADE. • Template2 is enabled and configured with sensitive column PERSON.ADDRESS. • Template3 is disabled and configured with sensitive column PERSON.DEPARTMENT. For a new event, data in the PERSON.NAME, PERSON.PAYGRADE and PERSON.ADDRESS fields will display as "***".

5

SQL Extended Events Auditing (Preview)

- Introduction
- SQL Extended Events Auditing templates

Introduction

SQL Server Extended Events allow users to gather information on the performance of their SQL database. Separate SQL Extended Events auditing templates must be defined for each SQL Server instance to be audited by Change Auditor.

NOTE:

- A Change Auditor SQL Server license is required for SQL Extended Events auditing.
- Managing SQL Extended Events auditing templates is only available to Change Auditor administrators or users that hold a custom Change Auditor role that includes the View_SQL_Template operation.

SQL Extended Events Auditing templates

To enable SQL Extended Events auditing in Change Auditor, you must create an auditing template. SQL Extended Events templates are created and managed through PowerShell commands. See the Change Auditor PowerShell Command User Guide for details.

The following Change Auditor facilities and events are available for SQL Extended events auditing.

Facility Name	Event Class
Admin Extended Events	Audit SQL Server Admin Extended Event
Analytic Extended Events	Audit SQL Server Analytic Extended Event
Operational Extended Events	Audit SQL Server Operational Extended Event

NOTE: Debug channel events are not supported.

6

SQL Searches/Reports

- Introduction
- Create custom SQL searches
- Create custom SQL Data Level searches
- Create custom SQL Extended Events searches (Preview)

Introduction

You can search, report and alert on changes to all SQL instances being audited or changes made to a specific SQL instance, SQL database, or SQL Server object.

This section explains how to create a custom SQL search using the What tab. For a description of the dialogs mentioned, see the online help.

NOTE: As a best practice, you should not have both SQL and SQL Data Level subsystems defined in a single search. When the SQL subsystem is included without filters, all SQL Data Level events will be included.

Create custom SQL searches

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

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

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

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

To search all SQL instances:

1. Open the Searches page.
2. In the explorer view (left pane), expand and select the folder where you want to save your search.
3. Click **New** to enable the Search Properties tabs across the bottom of the Searches page.
4. On the Info tab, enter a name and description for the search.
5. Open the What tab, expand **Add** and select **Subsystem | SQL**.
6. On the Add SQL Instance dialog, select **All SQL Instances.**

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

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

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

9 When this search is run, Change Auditor will search for the SQL events based on the search criteria specified on the What tab and display the results in a new search results page.

To search a specific SQL instance, database or object:

1 Open the Searches page.

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

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

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

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

6 On the Add SQL Instance dialog, select **This Object.**

7 When the **This Object** option is selected, you must fill in at least one of the following fields to define the SQL objects to include in the search:

- **Instance** - Enter the name of the SQL instance or click the browse button to the far right to select from a list. Selecting the browse button will display the Select a SQL Instance and Database dialog which provides a list of SQL instances and associated databases from which you can select the instance and database to be used. If you leave this field blank, Change Auditor will search for SQL events based on the entries made in the **DB** and/or **Object** fields for all audited SQL instances.
- **DB** - Enter the name of the SQL database to be used or use the browse button to the far right to select from a list. Selecting the browse button will display the Select a SQL Instance and Database dialog which provides a list of SQL instances and associated databases from which you can select the instance and database to be used. If you leave this field blank, Change Auditor will search for SQL events based on the entries made in the **Instance** and/or **Object** fields for all audited SQL databases.
- **Object** - Enter a SQL Server object to be included in the search definition. If you leave this field blank, Change Auditor will search for SQL events based on the entries made in the **Instance** and/or **DB** fields for all audited SQL Server objects.

Once you have specified the SQL instance, database and/or object to be included in the search definition, click **Add** to add it to the Selection list at the bottom of the dialog.

> **NOTE:** Select the **Exclude the Above Selection(s)** check box if you want to search for changes to all SQL instances EXCEPT those listed in the 'what' list.

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

8 Once you have selected the SQL instance, database and/or object to be included in the search, click **OK** to save your selection and close the dialog.

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

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

10 When this search is run, Change Auditor will search for the SQL events based on the search criteria specified on the What tab and display the results in a new search results page.

To search for a SQL instance that already has an audited SQL event in the database:

1 Open the Searches page.

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

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

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

5 Open the What tab, expand **Add with Events** and select **Subsystem | SQL**.

6 On the Add SQL Instance dialog, select an instance from the list and click the **Add** button to add it to the selection list at the bottom of the page.

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

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

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

9 When this search is run, Change Auditor will search for the SQL events based on the search criteria specified on the What tab and display the results in a new search results page.

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

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

11 When this search is run, Change Auditor will search for the SQL events based on the search criteria specified on the What tab and display the results in a new search results page.

Create custom SQL Data Level searches

The following scenarios explain how to use the What tab to create custom SQL Data Level searches.

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

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

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

To search a specific SQL Data Level object:

1 Open the Searches page.

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

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

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

5 Open the What tab, expand **Add** and select **Subsystem | SQL Data Level Events**.

6 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**

Once you have specified the search term, click **Add** to add it to the Selection list at the bottom of the dialog.

> **NOTE:** Select the **Exclude the Above Selection(s)** check box if you want to search for changes to all SQL Data Level events EXCEPT those that match the specified criteria.

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

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

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

9 When this search is run, Change Auditor will search for the SQL Data Level events based on the search criteria specified on the What tab and display the results in a new search results page.

Create custom SQL Extended Events searches (Preview)

The following scenarios explain how to use the What tab to create custom SQL Extended Events searches.

> **NOTE:** If you wanted to, you can use the other search properties tabs to define additional criteria:
>
> - Who - allows you to search for events generated by a specific user, computer or group
> - Where - allows you to search for events captured by a specific agent or within a specific domain or site
> - When - allows you to search for events that occurred within a specific date/time range
> - Origin - allows you to search for events that originated from a specific workstation or server

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

To search for a specific SQL Extended Events events:

1 Open the Searches page.

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

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

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

5 Open the What tab, and click **Add**.

You can then filter by facility or event class to locate SQL Extended Events.

6 Once you have specified the facility or event class, click **Add** to add it to the Selection list at the bottom of the dialog.

> **NOTE:** Select the **Exclude the Above Selection(s)** check box if you want to search for changes to all SQL Extended Events events EXCEPT those that match the specified criteria.

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

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

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

9 When this search is run, Change Auditor will search for the SQL Extended Events events based on the search criteria specified on the What tab and display the results in a new search results page.

7

Disabled SQL Events

This section provides an alphabetical list of the SQL events that are disabled by default in Change Auditor. If you want to audit for these events, use the Audit Events page on the Administration Tasks tab to enable these events.

Table 4. Disabled SQL events

Event Class disabled by default	Facility
Audit Add Login	SQL Security Audit Event
Audit Drop Login	SQL Security Audit Event
Audit Login Change	SQL Security Audit Event
Audit Change Audit - Audit Started	SQL Security Audit Event
Audit Change Audit - Audit Stopped	SQL Security Audit Event
Audit Create Object with Derived Permission	SQL Security Audit Event
Audit Drop Object with Derived Permission	SQL Security Audit Event
Audit Schema Object Access	SQL Security Audit Event
Audit Server Alter Trace	SQL Security Audit Event
Auto Stats - Async Completed	SQL Performance Event
Auto Stats - Async Queued	SQL Performance Event
Auto Stats - Async Starting	SQL Performance Event
Auto Stats - Sync	SQL Performance Event
Blocked Process Report	SQL Errors and Warnings Event
Broker: Message Classify - Delayed	SQL Broker Event
Degree of Parallelism - Delete	SQL Performance Event
Degree of Parallelism - Insert	SQL Performance Event
Degree of Parallelism - Select	SQL Performance Event
Degree of Parallelism - Update	SQL Performance Event
Error Logged	SQL Errors and Warnings Event
Event Logged	SQL Errors and Warnings Event
Exception	SQL Errors and Warnings Event
Exec Prepared SQL	SQL TSQL Event
Execution Warnings - Query Timeout	SQL Errors and Warnings Event
Execution Warnings - Query Wait	SQL Errors and Warnings Event
Lock: Acquired	SQL Locks Event
Lock: Cancel	SQL Locks Event
Lock: Escalation	SQL Locks Event
Lock: Released	SQL Locks Event
Lock: Timeout	SQL Locks Event
Lock: Timeout (timeout > 0)	SQL Locks Event
Object: Altered - Begin	SQL Objects Event
Object: Altered - Rollback	SQL Objects Event

Table 4. Disabled SQL events

Event Class disabled by default	Facility
Object: Altered - Commit	SQL Objects Event
Object: Created - Begin	SQL Objects Event
Object: Created - Commit	SQL Objects Event
Object: Created - Commit	SQL Objects Event
Object: Deleted - Begin	SQL Objects Event
Object: Deleted - Rollback	SQL Objects Event
Object: Deleted - Commit	SQL Objects Event
Performance Statistics - Cache Query Destroyed	SQL Performance Event
Performance Statistics - New Batch SQL Text	SQL Performance Event
Performance Statistics - Queries in Ad Hoc Statement Compiled	SQL Performance Event
Performance Statistics - Queries in Stored Procedure Compiled	SQL Performance Event
Prepare SQL	SQL TSQL Event
QN:Dynamics - Clock Run Finished	SQL Query Notifications Event
QN:Dynamics - Clock Run Started	SQL Query Notifications Event
QN:Dynamics - Master Cleanup Task Finished	SQL Query Notifications Event
QN:Dynamics - Master Cleanup Task Started	SQL Query Notifications Event
RPC:Completed	SQL Stored Procedures Event
RPC:Starting	SQL Stored Procedures Event
Scan:Started	SQL Scan Event
Scan:Stopped	SQL Scan Event
Showplan All	SQL Performance Event
Showplan All for Query Compile	SQL Performance Event
Showplan Statistics Profile	SQL Performance Event
Showplan Text	SQL Performance Event
Showplan Text (Unencoded)	SQL Performance Event
Showplan XML	SQL Performance Event
Showplan XML for Query Compile	SQL Performance Event
Showplan XML Statistics Profile	SQL Performance Event
SQL:BatchCompleted	SQL TSQL Event
SQL:BatchStarting	SQL TSQL Event
SQL:FullTextQuery	SQL Performance Event
SQL:StmtCompleted	SQL TSQL Event
SQL:StmtRecompile - Deferred Compile	SQL TSQL Event
SQL:StmtRecompile - Set Option Changed	SQL TSQL Event
SQL:StmtRecompile - Statistics Changed	SQL TSQL Event
SQL:StmtStarting	SQL TSQL Event
SQLTransaction Begin	SQL Transactions Event
SQLTransaction Commit	SQL Transactions Event
SQLTransaction Rollback	SQL Transactions Event
SQLTransaction Savepoint	SQL Transactions Event
SP:CacheHit - Compplan Hit	SQL Stored Procedures Event
SP:CacheHit - Execution Context Hit	SQL Stored Procedures Event

Table 4. Disabled SQL events

Event Class disabled by default	Facility
SP:CacheMiss	SQL Stored Procedures Event
SP:Completed	SQL Stored Procedures Event
SP:Recompile - Recompile DNR	SQL Stored Procedures Event
SP:Recompile - Set Option Changed	SQL Stored Procedures Event
SP:Recompile - Statistics Changed	SQL Stored Procedures Event
SP:Starting	SQL Stored Procedures Event
SP:StmtStarting	SQL Stored Procedures Event
TransactionLog	SQL Transactions Event
Unprepare SQL	SQL TSQL Event
User Error Message	SQL Errors and Warnings Event
XQuery Static Type	SQL TSQL Event

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.