Quest® Change Auditor for Authentication Services 7.1

User Guide

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.
4 Polaris Way
Aliso Viejo, CA 92656

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

Patents

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

Trademarks

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

Legend

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

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

Change Auditor for Authentication Services User Guide
Updated - December 2020
Software Version - 7.1

Contents

1

Quest Change Auditor for Authentication Services Overview

- Introduction
- Change Auditor for Authentication deployment requirements

Introduction

Authentication Services is patented technology that enables organizations to extend the security and compliance of Active Directory to UNIX, Linux, and Mac platforms and enterprise applications. Using Change Auditor, you can track, audit, report and alert on all critical changes to:

- Unix/Linux/Mac-related data for Active Directory users, groups, computers, NIS objects and Authentication Services personalities
- Unix/Linux/Mac settings in Group Policy Objects

Change Auditor for Authentication:

- Audits all critical changes.
- Tracks user activity.
- Turns irrelevant data into meaningful information to drive security and compliance.
- Automates reporting for corporate regulations.

This guide has been prepared to assist you in becoming familiar with Change Auditor for Authentication Services. 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 see the Change Auditor User Guide and the Change Auditor Installation Guide.
- For event details, see the Change Auditor for Authentication Services Event Reference Guide.

Change Auditor for Authentication deployment requirements

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

> **NOTE:** Authentication Services auditing is only available if you have licensed Change Auditor for Active Directory. 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.**

2

Getting Started

- Deployment requirements
- Enable Authentication Services auditing
- Enable and disable events as required
- Make changes and run a report

Deployment requirements

> **NOTE:** After an agent upgrade from version 7.0.4 or earlier, you will need to update your configuration setup to enable Authentication Services auditing where required.

To capture activity performed with Authentication Services you need to:

- Ensure that Authentication Services 4.0 (or later) is properly installed and configured.
- Enable Authentication Services auditing through the agent configuration setup.
- Deploy agents on all Active Directory domain controllers in the forest to capture modifications to the Authentication Services configuration container.
- Enable and disable the required events.

Enable Authentication Services auditing

Authentication Services auditing is enabled and disabled on a configuration basis from through the configuration setup.

To enable Authentication Services auditing:

1. Open the Administration Tasks tab and click **Configuration**.
2. Select **Agent** in the Configuration task list.
3. From the Agent Configuration page, click **Configurations** to see the available configuration definitions. From here you can edit a configuration to include Authentication Services or create a new configuration.
4. Select the required agent configuration, select the **Authentication Services** tab, and click the option to enabled auditing.

Enable and disable events as required

You can enable or disable events to best suit your organization. To view or modify the current event auditing settings, use the Audit Events page, which is accessible through the Administration Tasks tab.

To disable/enable individual events:

1. Open the Administration Tasks tab.
2. Click **Auditing**.
3. Select **Audit Events** (under the Configuration heading in the Auditing task list) to display the Audit Events page.
4. To disable an event, use one of the following methods:
   - Select one or more enabled events and click **Disable**. (Use the **Shift** or **Ctrl** keys to select multiple events.)
   - Select an enabled event, place your cursor in the corresponding **Status** cell, click the arrow control and select **Disabled** from the drop-down menu.
   - Right-click an enabled event and select **Disable**.

5 To enable an event, use one of the following methods:

- Select one or more disabled events and click **Enable**. (Use the **Shift** or **Ctrl** keys to select multiple events.)
- Select a disabled event, place your cursor in the corresponding **Status** cell, click the arrow control and select **Enabled** from the drop-down menu.
- Right-click a disabled event and select **Enable**.

> **NOTE:** You can also disable or enable an event using the **Disable/Enable** tool bar button at the top of the Event Details pane on a Search Results page.

Make changes and run a report

1 To test Authentication Services auditing, make some changes to the host being monitored.

For example:

- change the Unix name of a Unix-enabled Active Directory group
- rename an NIS object within Active Directory
- move an Authentication Services computer object in an Active Directory domain

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 | Authentication Services** folder in the left pane.

5 Locate and double-click **All Authentication Services events in last 30 days**.

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

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

3

Authentication Services Searches/Reports

- Introduction
- Authentication Services built-in reports
- Create custom searches
- Search results

Introduction

You can use predefined reports to retrieve valuable change information from a variety of perspectives.

> ℹ **NOTE:** The terms ‘searches’ and ‘reports’ are used in conjunction to acquire the desired output. You run a ‘search’ and the results returned are referred to as a ‘report’.

You can also create custom search definitions to search for the configuration changes that need to be tracked in your environment. You will use the search properties tabs across the bottom of the Searches page to define new custom searches.

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

Authentication Services built-in reports

To see a complete list of built-in reports, see the Change Auditor Built-in Reports Reference Guide.

To run a built-in search:

1. Click on the **Searches** tab or select **View | Searches**.
2. Expand and select the appropriate folder in the explorer view (left-hand pane) to display the list of search definitions stored in the selected folder. For example, selecting the **Shared | Built-in | Authentication Services** will display all the built-in searches available for One Identity Authentication Services.
3. In the right-hand pane, locate the search to be run and use one of the following methods to run the selected search:
   - Double-click a search definition
   - Right-click a search definition and select the **Run** menu command
   - Select the search definition and click the **Run** tool bar button at the top of the Searches page
4. A new Search Results Page will be displayed populated with the audited events that met the search criteria defined in the selected search definition.

> ℹ **NOTE:** To modify a built-in search or create a custom Authentication Services search, see the Change Auditor User Guide.

Create custom searches

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

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

To search for a specific event class:

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

   Selecting the **Private** folder will create a search that only you can run and view, whereas selecting the **Shared** folder will create a search which can be run and viewed by all Change Auditor users.
3. Click **New** at the top of the Searches page.

   This will activate the Search Properties tabs across the bottom of the Searches page.
4. On the Info tab, enter a name and description for the search.
5. Open the What tab, click **Add** (or expand the **Add** tool bar button and select **Event Class**).
6. On the Add Facilities or Event Classes dialog, enter **Authentication Services Monitoring** in the data filter field under the Facility heading to display all of the Authentication Services events.
7. From this list, select one or more events and use the **Add | Add This Event** option to add the selected events to the list box at the bottom of the dialog. Click **OK** to save your selection and close the dialog.
8. Click **Run** to save and run the search. Click **Save** to save the search definition without running it.
9. When this search runs, Change Auditor searches for the Authentication Services events based on the search criteria specified on the What tab and display the results in a new search results page.

Search results

The event information (including key information like who, what, when, where, why, the event origin, and the file information) can be viewed on the Event Details pane.

Table 1. Event Details pane: Authentication Services events

ChangeAuditor	Description
Severity	Displays “Low”, “Medium”, or “High” depending on the event.
Who	Specifies the name of the user who initiated the change.
When	Specifies the date and time when the change occurred.
Where	Displays the name of the workstation where the change occurred.
Source	Displays ‘Change Auditor’ which is the application from which the event was retrieved.
Origin	Displays the NetBIOS name and IP address of the workstation from which the event was generated.
What	Displays a description of the activity that occurred. **NOTE:** For lengthy descriptions, hover your cursor over the description field to view the entire event description.
Facility	Displays that it is Authentication Services Monitoring activity.

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 Office 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.