Quest

Quest® Change Auditor for Authentication Services 7.6

Event Reference 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 Software, 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 Authentication Services Event Reference Guide
Updated - July 2025
Software Version - 7.6

Contents

Introduction **4**

Change Auditor for Authentication Services Events **5**
Authentication Services Monitoring 5

Built-in Reports **7**
Authentication Services built-in reports 7

About us **9**
Our brand, our vision. Together. 9
Contacting Quest 9
Technical support resources 9

1

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

NOTE: Authentication Services auditing is only available when you have Authentication Services 4.0 (or later) installed and a Change Auditor for Active Directory license.

This guide lists the events that can be captured by Change Auditor for Authentication Services. Separate event reference guides are provided that list the core Change Auditor events (when any Change Auditor license is applied) and the events captured when the different auditing modules are licensed.

2

Change Auditor for Authentication Services Events

Change Auditor for Authentication Services queries Active Directory for modifications made to the Authentication Services configuration container. This section lists the audited events captured by Change Auditor for Authentication Services. They are listed in alphabetical order by facility.

IMPORTANT: When expecting large numbers of events, it may be necessary to increase the Max Events per Connection setting in the client (Agent Configuration on the Administration Tasks tab) to avoid an ever-increasing backlog of events waiting to be sent from the agent to the coordinator database.

NOTE: To view a complete list of all the Change Auditor events, open the Audit Events page on the Administration Tasks tab in the client. This page contains a list of all the events available for auditing by Change Auditor. It also displays the facility to which the event belongs, the severity assigned to each event, if the event is enabled or disabled, and the type of Change Auditor license that is required to capture each event.

Authentication Services Monitoring

Table 1. Authentication Services Monitoring events

Event	Description	Severity
Authentication Services Computer Object Added	Created when a new Authentication Services computer object is added to an Active Directory domain.	Medium
Authentication Services Computer Object Attribute Changed	Created when an attribute for an Authentication Services computer object is changed.	Medium
Authentication Services Computer Object Deleted	Created when an Authentication Services computer object is removed from an Active Directory domain.	Medium
Authentication Services Computer Object Moved	Created when an Authentication Services computer object is moved in an Active Directory domain.	Medium
Authentication Services Computer Object Renamed	Created when an Authentication Services computer object is renamed in an Active Directory domain.	Medium
Authentication Services GPO Setting Changed	Created when an Authentication Services group policy settings is changed.	Medium
NIS Object Added	Created when an NIS object is added to Active Directory.	Medium
NIS Object Attribute Changed	Created when the data stored in an NIS object in Active Directory is changed.	Medium
NIS Object Deleted	Created when an NIS object is deleted from Active Directory.	Medium
NIS Object Moved	Created when an NIS object is moved within Active Directory.	Medium
NIS Object Renamed	Created when an NIS object is renamed within Active Directory.	Medium

Table 1. Authentication Services Monitoring events

Event	Description	Severity
Personality Object Added	Created when a UNIX user or group personality object is added to Active Directory.	Medium
Personality Object Attribute Changed	Created when the data stored in a Unix personality object in Active Directory is changed.	Medium
Personality Object Deleted	Created when a Unix user or group personality object is deleted from Active Directory.	Medium
Personality Object Moved	Created when a Unix personality object is moved within Active Directory.	Medium
Personality Object Renamed	Created when a Unix personality object is renamed within Active Directory.	Medium
UNIX GECOS Changed	Created when the GECOS attribute of a Unix-enabled Active Directory user is changed.	Medium
UNIX Group ID Number Changed for Group	Created when the group ID number of a Unix-enabled Active Directory group is changed.	Medium
UNIX Group ID Number Changed for User	Created when the primary group ID number of a Unix-enabled Active Directory user is changed.	Medium
UNIX Group Name Changed	Created when the Unix name of a Unix-enabled Active Directory group is changed.	Medium
UNIX Home Directory Changed	Created when the Unix home directory of a Unix-enabled Active Directory user is changed.	Medium
UNIX Login Name Changed	Created when the Unix login name of a Unix-enabled Active Directory user is changed.	Medium
UNIX Login Shell Changed	Created when the Unix login shell of a Unix-enabled Active Directory user is changed.	Medium
UNIX User ID Number Changed	Created when the user ID number of a Unix-enabled Active Directory user is changed.	Medium
UNIX-Enabled Changed for Group	Created when the Unix attributes of an Active Directory group are changed such that it no longer exists on a Unix or Linux® system.	Medium
UNIX-Enabled Changed for User	Created when the Unix attributes of an Active Directory user are changed such that it no longer exists on a Unix or Linux system.	Medium
UNIX-Enabled Group Created	Created when a new Active Directory group with configured Unix attributes is created.	Medium
UNIX-Enabled Group Deleted	Created when a Unix-enabled Active Directory group is deleted.	Medium
UNIX-Enabled User Created	Created when a new Active Directory user with configured Unix attributes is created.	Medium
UNIX-Enabled User Deleted	Created when a Unix-enabled Active Directory user is deleted.	Medium

3

Built-in Reports

Change Auditor provides predefined reports which allow you to quickly retrieve valuable change information from a variety of perspectives.

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’.

To run a built-in search:

1. Click on the **Searches** tab or select the **View | Searches** menu command or **Ctrl+F10** to open the Searches page.
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 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.

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

Authentication Services built-in reports

The following built-in reports are available:

- All Authentication Services events in last 30 days
- Authentication Services computer object auditing in last 30 days
- Authentication Services computers added in last 30 days
- Authentication Services computers deleted in last 30 days
- Authentication Services GPO settings changes in last 30 days
- Groups set to UNIX-disabled in last 30 days
- Groups set to UNIX-enabled and created in last 30 days
- Groups set to UNIX-enabled in last 30 days
- NIS object auditing in last 30 days
- Personality object auditing in last 30 days
- UNIX home directory changed in last 30 days
- UNIX login shell changed in last 30 days

- UNIX-enabled groups created in last 30 days
- UNIX-enabled groups deleted in last 30 days
- UNIX-enabled users created in last 30 days
- UNIX-enabled users deleted in last 30 days
- Users set to UNIX-disabled in last 30 days
- Users set to UNIX-enabled and created in last 30 days
- Users set to UNIX-enabled in last 30 days

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.