

Quest® Change Auditor for Logon Activity 7.3
Event Reference Guide



© 2022 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.
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 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.

Contents

Introduction	4
Change Auditor for Logon Activity Events	5
Active Directory Federation Services - Sign-in	5
Authentication Activity	6
Azure Active Directory Sign-Ins	7
Azure Active Directory Sign-in Risk Event	7
Domain Controller Authentication	8
Logon Session	8
About us	10
Our brand, our vision. Together.	10
Contacting Quest	10
Technical support resources	10

Introduction

Information about login and log out activity is important for regulatory compliance and user activity tracking. There are two auditing modules provided to allow you to collect this important activity:

- The Change Auditor for Logon Activity User auditing module enables server agents to generate the following events:
 - Authentication activity (interactive, remote interactive and network logins) including successful and failed logins performed on monitored servers
 - Domain Controller authentication activity (Kerberos), including successful and failed requests (Domain Controller agents only)
 - User log on session activity (the actual time spent on a server)
- The Change Auditor for Logon Activity Workstation auditing module enables workstation agents to generate the following events:
 - Authentication activity (interactive, remote interactive and network logins), including successful and failed logins performed on monitored workstations
 - User log on session activity (the actual time spent on a workstation)

i | **NOTE:** Network login and successful domain authentication (Kerberos) events are disabled by default and must first be enabled in the client before they are captured. Use the Audit Events page on the Administration Tasks tab to enable events.

i | **NOTE:** Starting with Change Auditor 6.5, these auditing modules eliminate the dependency on Quest InTrust and the Change Auditor Data Gateway Service to capture login activity.

This guide lists the events captured by these two Change Auditor for Logon Activity auditing modules. Separate event reference guides are available 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.

Change Auditor for Logon Activity Events

This section lists the audited events captured by the two Change Auditor for Logon Activity auditing modules. They are listed in alphabetical order by facility:

- [Active Directory Federation Services - Sign-in](#)
- [Authentication Activity](#)
- [Azure Active Directory Sign-Ins](#)
- [Azure Active Directory Sign-in Risk Event](#)
- [Azure Active Directory Sign-in Risk Event](#)
- [Logon Session](#)

i | **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.

i | **NOTE:** To view a complete list of all 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 license that is required to capture each event.

Active Directory Federation Services - Sign-in

Table 1. Active Directory Federation Services - Sign-in events

Event	Description	Severity
Failed Active Directory Federation Services sign-in	Created when a user fails to sign in using Active Directory Federation Services.	Medium
Successful Active Directory Federation Services sign-in	Created when a user successfully signs in using Active Directory Federation Services.	Low

Authentication Activity

i **IMPORTANT:** To capture Authentication Activity events, you must first enable (that is, set to Success,Failure) the 'Audit Logon events' audit policy for all servers and workstations.

Domain - Group Policy:

- Default Domain Policy\Computer Configuration\Windows Settings\Security Settings\Local Policies\Audit Policy\Audit logon events

Workgroup - Local Group Policy:

- Local Computer Policy\Computer Configuration\Windows Settings\Security Settings\Local Policies\Audit Policy\Audit logon events

i **NOTE:** Authentication Activity events for servers are available with the Change Auditor for Logon Activity User auditing module. Authentication Activity events for workstations require the Change Auditor for Logon Activity Workstation auditing module and workstation agents to be deployed to the workstations to be monitored.

Table 2. Authentication Activity events

Event	Description	Severity
User failed to log on interactively	Created when a user failed to log on interactively to a computer. Windows Event equivalent: 529/4625	Medium
User failed to log on interactively from a remote computer	Created when a user failed to log on interactively from a remote computer. Windows Event: 529/4625	Medium
User failed to perform a network logon from a remote computer	Created when a user failed to log on from a remote computer on the network. (Disabled by default) Windows Event equivalent: 529/4625	Medium
User logged on interactively	Created when a user successfully logged on interactively to a computer. Windows Event equivalent: 528/4624 NOTE: When logging onto a monitored Windows 2012 or 2012 R2 server or a Windows 8.1 workstation, you may see additional events with 'Windows Manager\DWM-n' in the who information. This is expected behavior because the logon is being performed by the system.	Medium
User logged on interactively from a remote computer	Created when a user successfully logged on interactively from a remote computer. Windows Event equivalent: 528/4624	Medium
User performed a successful network logon from a remote computer	Crated when a user successfully logged on from a remote computer on the network. (Disabled by default) Windows Event equivalent: 540/4624	Medium
User performed a successful NTLM V1 logon	Created when a user successfully logged into server through NTLM V1. (Disabled by default)	Medium
User performed a successful NTLM V2 logon	Created when a user successfully logged into server through NTLM V2. (Disabled by default)	Low

Azure Active Directory Sign-Ins

Change Auditor audits activities in the Azure Active Directory that correspond to the events in the Sign-ins report in the Azure Active Directory portal.

Table 3. Azure Active Directory Sign-in events

Event	Description	Severity
Failed Azure Active Directory sign-in	Created when a user fails to sign-in to an application. The event details show the user whose attempt failed, their location, and the application they attempted to access.	Medium
Successful Azure Active Directory sign-in	Created when a user successfully signs-in to an application. The event details show the user whose attempt failed, their location, and the application they attempted to access.	Low
Azure Active Directory - sign-in event	Generic sign-in event with a dynamically constructed event description (What statement). The event is created when sign-in activity is detected that does not have a corresponding event defined in Change Auditor.	Low

Azure Active Directory Sign-in Risk Event

Change Auditor audits activities in the Azure Active Directory that correspond to the events in the Risky sign-ins report in the Azure Active Directory portal.

Table 4. Azure Active Directory Sign-in risk events

Event	Description	Severity
Active risk event detected	Created when a new risk event is detected with an active state.	High
Active risk event status changed to closed	Created when an active risk event is closed as a result of being marked as: <ul style="list-style-type: none">Resolved: The issue has been addressed and has been safely closed.False positive: The issue has been incorrectly identified as a risk and has been safely closed.Ignore: The issue has been removed from the active list. This event helps you to understand why a risk event has been manually closed.	Low
Closed risk event status changed to active	Created when a closed risk event is reactivated.	High
Closed risk event detected	Created when a new risk event is detected with a closed state. This can happen if the risk event has been marked as resolved, a false positive, set to ignore, closed (remediated), closed (login blocked), closed (automatic multi-factor authentication), or closed (multiple reasons) before it has been detected by Change Auditor for the first time.	Low

Domain Controller Authentication

- NOTE:** Domain Controller Authentication events are only available with the Change Auditor for Logon Activity User auditing module. They are not available with the Change Auditor for Logon Activity Workstation auditing module.
- NOTE:** The following Domain Controller Authentication events do not require Windows system provided auditing enabled and are recorded in Change Auditor even if they are not recorded in the Windows Event log:
 - User authenticated through Kerberos
 - User failed to authenticate through Kerberos

Table 5. Domain Controller Authentication events

Event	Description	Severity
A Kerberos service ticket was created with an unsafe encryption type	This event is created when a Kerberos service ticket was created for a service with weak encryption type: not AES.	High
Kerberos user ticket that exceeds the maximum ticket lifetime detected	A Kerberos user ticket can be used to verify your identity and gain access to specific resources or services in your domain. A golden ticket is a forged Kerberos ticket. An attack using a golden ticket is extremely dangerous due to the forged identity, elevated access it allows, and because it can be reused over its lifetime (10 years by default). This event is created when the Kerberos Ticket Lifetime value in agent configuration is exceeded indicating a possible golden ticket attack.	High
User authenticated through Kerberos	Created when a user successfully authenticated to a domain controller using Kerberos authentication. (Disabled by default)	Medium
User failed to authenticate through Kerberos	Created when a user failed to authenticate to a domain controller using Kerberos authentication.	Medium
User authenticated through NTLM	Created when a user successfully authenticated to a domain controller using NTLM authentication. (Disabled by default)	Low
User failed to authenticate through NTLM	Created when a user failed to authenticate to a domain controller using NTLM authentication.	Medium

Logon Session

- NOTE:** Logon Session events for servers are available with the Change Auditor for Logon Activity User auditing module. Logon Session events for workstations require the Change Auditor for Logon Activity Workstation auditing module and workstation agents to be deployed to the workstations to be monitored.

Table 6. Logon Session events

Event	Description	Severity
A user session took place	Created when a user session took place on a monitored computer.	Medium
A user session was ended by the screensaver turning on	Created when a user session is ended because the screensaver turned on.	Medium
A user session was ended by user locking the computer	Created when a user session is ended because the user locked up the computer.	Medium

Table 6. Logon Session events

Event	Description	Severity
A user session was ended by user logging off	Created when a user session is ended because the user logged off.	Medium
A user session was ended by user stopping a terminal services connection	Created when a user session is ended because the user stopped a terminal services connection.	Medium
A user session was ended due to computer shutdown	Created when a user session is ended because a user has shut down or restarted the computer.	Medium
A user session was ended due to user switch	Created when a user session is ended because a different user has logged on.	Medium
A user session was started	Created when a user session is started on a monitored computer.	Medium
A user session was started before the start of the user session monitoring service	Created when a new user session is started before the user session monitoring service is started.	Medium
A user session was started by user exiting screensaver mode	Created when a new user session is started because the user exited the screensaver mode.	Medium
A user session was started by user making a terminal services connection	Created when a new user session is started because a user logged in through a terminal services connection.	Medium
A user session was started by user unlocking the computer	Created when a new user session is started because the user unlocked the computer.	Medium
A user session was started due to user switch	Created when a new user session is started because a different user has logged on.	Medium
An incorrectly finished user session was found	Created when an incorrectly finished user session is found when the user session monitoring service is started.	Medium

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.