Quest®Change Auditor for Windows® File Servers 7.0

Event Reference Guide

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.

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

Change Auditor for Windows File Servers Event Reference Guide
Updated - May 2018
Software Version - 7.0

Contents

1

Introduction

Change Auditor for Windows File Server tracks, audits and alerts on file and folder changes in real time, translating events into simple text and eliminating the time and complexity required by native auditing. The auditing scope can be set on an individual file or folder or an entire file system recursive or non-recursive. You can also include or exclude certain files or folders from the audit scope in order to ensure a faster and more efficient audit process.

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

NOTE: File System auditing and event logging are only available if you have licensed Change Auditor for Windows File Server and have applied custom File System Auditing templates that define the files/folders to be audited. Contact your Sales Representative for more information on obtaining Change Auditor for Windows File Server.

This guide lists the events that can be captured by Change Auditor for Windows File Server. 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 Windows File Server Events

This section lists the audited events captured when Change Auditor for Windows File Server is licensed and custom file system auditing templates are applied to Change Auditor agents defining the files/folders to be audited. These events 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 events, open the Audit Events page on the Administration Tasks tab in the client. This page 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 for Windows File Server license that is required to capture each event.

Custom File Systems Monitoring

NOTE: Events are generated as described below when actions are taken on folders that have subordinate files and folders:

- **Moving a parent folder:** For a 'Move' operation, only **one** event will be generated for the parent folder because action is only on the parent folder's path, none of the child folders or files are physically moved.
- **Deleting a parent folder:** For a 'Delete' operation, an event will be generated for each folder or file because each object will be removed separately.
- **Copying a parent folder:** For a 'Copy' operation, an event will be generated for each folder and file because a new object will be created within the target folder.

If a parent folder is copied to a target folder that is not being monitored, no event will be generated. The target folder must be monitored in order for an event to be generated.

Table 1. Custom File Systems Monitoring events

Event	Description	Severity
Failed File Access (NTFS Permissions)	Created when access to a file is denied based on the NTFS permissions assigned.	Medium
Failed File Access (Change Auditor Protection)	Created when access to a file is denied because it is locked down using the File System Protection feature of Change Auditor.	Medium
Failed Folder Access (NTFS Permissions)	Created when access to a folder is denied based on the NTFS permissions assigned.	Medium
Failed Folder Access (Change Auditor Protection)	Created when access to a folder is denied because it is locked down using the File System Protection feature of Change Auditor.	Medium
Failed Share Access (NTFS Permissions)	Created when access to a file share properties is denied based on the NTFS permissions assigned. **NOTE:** This event monitors changes made to a share's properties (such as share permissions and comments). It does NOT monitor failed access to a share from a remote computer. If a user tries to read or change a share's property, the event will be triggered.	Medium
Failed Share Access (Change Auditor Protection)	Created when access to a file share properties is denied because it is locked down using the File System Protection feature of Change Auditor. **NOTE:** Once you have a share protected, only attempts to change a share's property will generate the 'failed share access' event; not attempts to access the share itself.	Medium
File Access Rights Changed	Created when file access rights have changed on a file system. **NOTE:** Change Auditor access control list (ACL) events, i.e., discretionary access control list (DACL) and system access control list (SACL) changes, will not report inherited access control entry (ACE) changes. This event does NOT report inherited ACL changes.	Medium
File Attribute Changed	Created when a file attribute has changed on a file system.	Medium
File Auditing Changed	Created when file auditing has changed on a file system. **NOTE:** Change Auditor access control list (ACL) events, i.e., discretionary access control list (DACL) and system access control list (SACL) changes, will not report inherited access control entry (ACE) changes. This event does NOT report inherited ACL changes.	Medium
File Central Access Policy Changed	Created when the central access policy of a file changed on a file system. **NOTE:** Central Access Policy is available in Windows Server 2012; therefore, this event does not apply to earlier versions of Windows Server.	Medium
File Classification Changed	Created when the classification of a file changed on a file system. **NOTE:** File Classification is available in Windows Server 2012; therefore, this event does not apply to earlier versions of Windows Server.	Medium
File Created	Created when a file is created on a file system.	Medium
File Deleted	Created when a file is deleted on a file system.	Medium
File Last Write Changed	Created when the last write time of a file is changed on a file system.	Medium
File Moved	Created when a file is moved on a file system.	Medium

Table 1. Custom File Systems Monitoring events

Event	Description	Severity
File Opened	Created when a file is opened on a file system.	Medium
File Ownership Changed	Created when file ownership is changed on a file system.	Medium
File Renamed	Created when a file is renamed on a file system.	Medium
Folder Access Rights Changed	Created when folder access rights have changed on a file system. **NOTE:** Change Auditor access control list (ACL) events, i.e., discretionary access control list (DACL) and system access control list (SACL) changes, will not report inherited access control entry (ACE) changes. This event does NOT report inherited ACL changes.	Medium
Folder Attribute Changed	Created when a folder attribute has changed on a file system.	Medium
Folder Auditing Changed	Created when folder auditing has changed on a file system. **NOTE:** Change Auditor access control list (ACL) events, i.e., discretionary access control list (DACL) and system access control list (SACL) changes, will not report inherited access control entry (ACE) changes. This event does NOT report inherited ACL changes.	Medium
Folder Central Access Policy Changed	Created when the central access policy of a folder changed on a file system. **NOTE:** Central Access Policy is available in Windows Server 2012; therefore, this event does not apply to earlier versions of Windows Server.	Medium
Folder Classification Changed	Created when the classification of a folder changed on a file system. **NOTE:** File Classification is available in Windows Server 2012; therefore, this event does not apply to earlier versions of Windows Server.	Medium
Folder Created	Created when a folder is created on a file system.	Medium
Folder Deleted	Created when a folder is removed from a file system.	Medium
Folder Moved	Created when a folder is moved on a file system.	Medium
Folder Opened	Created when a folder is opened on a file system.	Medium
Folder Ownership Changed	Created when folder ownership has changed on a file system.	Medium
Folder Renamed	Created when a folder is renamed on a file system.	Medium
Junction Point Created	Created when a third-party tool is installed and a new junction point is created.	Medium
Junction Point Deleted	Created when a third-party tool is installed and a junction point is deleted.	Medium
Local Share Added	Created when a local share is added to a file system.	Medium
Local Share Folder Path Changed	Created when the path of a local share folder is changed on a file system.	Medium
Local Share Permissions Changed	Created when local share permissions are changed on a file system.	Medium
Local Share Removed	Created when a local share is removed from a file system.	Medium
Shadow Copy Created	Created when a shadow copy is created for a volume. Disabled by default.	Medium
Shadow Copy Deleted	Created when a shadow copy is deleted from a volume. Disabled by default.	Medium

Table 1. Custom File Systems Monitoring events

Event	Description	Severity
Shadow Copy Rolled Back	Created when a shadow copy for a volume is rolled back. Disabled by default.	Medium
Transaction Status Changed	Created when the status of the transaction changed. Disabled by default. **NOTE:** Transaction Status events are only supported on Windows Server 2008 or newer OS.	Medium

3

Log Events

When event logging for File System is enabled, Windows File Server events will also be written to a Windows event log, named Quest File Access Audit event log. These log events can then be gathered by InTrust and Quest Knowledge Portal for further processing and reporting.

NOTE: To enable event logging, select **Event Logging** on the Agent Configuration page (Administration Tasks tab), and select the type of event logging to enable.

Quest File Access Audit event log

The following table lists the Windows File Server events that are recorded to the Quest File Access Audit event log when File System event logging is enabled in Change Auditor. They are listed in numeric order by event ID.

Table 2. Quest File Access Audit event log events

Event ID	Description
1	File audit service started
2	File audit service stopped
3	File audit service error
4	File audit service configuration changed
5	File audit service abnormal termination
6	File audit service startup changed from Automatic
7	Disabled in safe mode
8	Protected folder move
257	Remote access failed (NTFS)
258	Local access failed (NTFS)
273	Remote object permissions changed
274	Local object permissions changed
769	Remote file read
770	Local file read
779	Remote folder open
780	Local folder opened
1025	Remote file written
1026	Local file written
1281	Remote object created
1282	Local object created
1537	Remote object deleted
1538	Local object deleted
1793	Remote object moved

Table 2. Quest File Access Audit event log events

Event ID	Description
1794	Local object moved
2049	Remote object renamed
2050	Local file renamed
2059	Remote object attribute changed
2060	Local object attribute changed
2069	Remote object auditing changed
2070	Local object auditing changed
2305	Remote object owner changed
2306	Local object owner changed
2561	Remote share settings change failed
2562	Local share settings changed failed
2817	Remote share created
2818	Local share created
3073	Remote share deleted
3074	Local share deleted
3329	Remote share permissions changed
3330	Local share permissions changed
4098	Local transaction status changed
4353	Remote access failed (lockdown)
4354	Local access failed (lockdown)
4610	Shadow copy created
4866	Shadow copy deleted
5122	Shadow copy rolled back
5200	Junction Point created
5210	Local Junction Point deleted
5211	Remote Junction Point deleted

About us

We are more than just a name

We are on a quest to make your information technology work harder for you. That is why we build community-driven software solutions that help you spend less time on IT administration and more time on business innovation. We help you modernize your data center, get you to the cloud quicker and provide the expertise, security and accessibility you need to grow your data-driven business. Combined with Quest's invitation to the global community to be a part of its innovation, and our firm commitment to ensuring customer satisfaction, we continue to deliver solutions that have a real impact on our customers today and leave a legacy we are proud of. We are challenging the status quo by transforming into a new software company. And as your partner, we work tirelessly to make sure your information technology is designed for you and by you. This is our mission, and we are in this together. Welcome to a new Quest. You are invited to Join the Innovation™.

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.