Quest

Quest® Change Auditor 7.6.3

Event Reference Guide

© 2026 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.
10801 N. Mopac Expressway
Building 3, Suite 400
Austin, TX 78759

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 Event Reference Guide
Updated - August 2026
Software Version - 7.6.3

Contents

Introduction **4**

Change Auditor Events **5**
Change Auditor Internal Auditing 5
Custom Registry Monitoring 26
Fault Tolerance 27
Local Group Monitoring 27
Local User Monitoring 28
Service Monitoring 30
System Events 31
Threat Detection Events 32

Log Events **34**
Change Auditor Coordinator Service event log 34
Change Auditor Service event log 44
Registry events 45
Local Groups events 45
Service events 46

About us **48**
Our brand, our vision. Together. 48
Contacting Quest 48
Technical support resources 48

1

Introduction

Change Auditor provides total auditing and security coverage for the enterprise including Active Directory, Exchange, Microsoft 365 Exchange, Microsoft Entra ID, Windows file servers, SQL Server, NetApp filers, EMC file servers, and SharePoint.

Change Auditor audits the activities taking place in your infrastructure and, with real-time alerts, delivers detailed information about vital changes and activities as they occur. Instantly know who made changes including the IP address of the originating workstation, where and when it occurred along with before and after values. Then automatically turn that information into intelligent, in-depth forensics for auditors and management — and reduce the risks associated with day-to-day operations.

Change Auditor uses a modular approach which allows for separate product deployment and management for key environments including:

- Active Directory
- Active Directory Query
- EMC
- Exchange
- Logon Activity
- NetApp
- SharePoint
- SQL Server
- Windows File Servers

NOTE: Each of these modules require a separate license to capture their associated events.

Additional Change Auditor auditing modules allow you to track, audit, report and alert on critical changes made using the following Quest products:

- Authentication Services
- Defender

In addition to real-time event auditing, you can also enable event logging to capture many of the Change Auditor events locally in a Windows event log. These event logs can then be collected using InTrust to satisfy long-term storage requirements.

This guide lists the core audited events available in Change Auditor regardless of the Change Auditor product license that is applied. Separate event reference guides are provided which list the additional events that are available for the different Change Auditor auditing modules.

2

Change Auditor Events

This section lists the audited events available in Change Auditor regardless of the applied Change Auditor product license. Audited events are listed in alphabetical order by facility:

- Change Auditor Internal Auditing
- Custom Registry Monitoring
- Fault Tolerance
- Local Group Monitoring
- Local User Monitoring
- Service Monitoring
- System Events

IMPORTANT: When expecting large numbers of events, it may be necessary to increase the Max Events per Connection settings 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. 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 license that is required to capture each event.

Change Auditor Internal Auditing

Table 1. Change Auditor Internal Auditing events

Event	Description	Severity
A Change Auditor license has expired	Created when a Change Auditor license expires.	High
A Change Auditor license will expire soon	Created 30 days prior to the date when a Change Auditor license is set to expire.	Medium
Active Directory Federation Services auditing template added	Created when an Active Directory Federation Services auditing template is added.	Medium
Active Directory Federation Services auditing template added to agent configuration	Created when Active Directory Federation Services auditing template is added to an agent configuration.	Low
Active Directory Federation Services auditing template disabled	Created when an Active Directory Federation Services auditing template is disabled.	Medium
Active Directory Federation Services auditing template enabled	Created when an Active Directory Federation Services auditing template is enabled.	Medium
Active Directory Federation Services auditing template removed	Created when an Active Directory Federation Services auditing template is removed.	Medium

Table 1. Change Auditor Internal Auditing events

Event	Description	Severity
Active Directory Federation Services auditing template removed from agent configuration	Created when Active Directory Federation Services auditing template is removed from an agent configuration.	Low
Active Directory Federation Services configuration changes auditing disabled	Created when an Active Directory Federation Services configuration changes auditing is disabled.	Medium
Active Directory Federation Services configuration changes auditing enabled	Created when an Active Directory Federation Services configuration changes auditing is enabled.	Medium
Active Directory Federation Services sign-in auditing enabled	Created when an Active Directory Federation Services sign-in auditing is enabled.	Medium
Active Directory Federation Services sign-in auditing disabled	Created when an Active Directory Federation Services sign-in auditing is disabled.	Medium
Active Directory Protection Template Added	Created when an Active Directory protection template is added to Change Auditor.	Medium
Active Directory Protection Template Changed	Created when an attribute is added or removed from the Active Directory protection template.	Medium
Active Directory Protection Template Disabled	Created when an Active Directory protection template is disabled.	Medium
Active Directory Protection Template Enabled	Created when an Active Directory protection template is enabled.	Medium
Active Directory Protection Template Removed	Created when an Active Directory protection template is removed from Change Auditor.	Medium
AD Query Container Added	Created when a container is added to the Excluded AD Query list.	Medium
AD Query Container Disabled	Created when a container is disabled on the Excluded AD Query list.	Medium
AD Query Container Enabled	Created when a container is enabled on the Excluded AD Query list.	Medium
AD Query Container Removed	Created when a container is removed from the Excluded AD Query list.	Medium
ADAM Attribute Severity Changed	Created when the severity for a monitored ADAM (AD LDS) attribute is changed.	Low
ADAM Monitoring Point Added	Created when an ADAM (AD LDS) instance and associated object classes are added to the Change Auditor auditing scope.	Low
ADAM Monitoring Point Removed	Created when an ADAM (AD LDS) instance and associated object classes are removed from the Change Auditor auditing scope.	Low
ADAM Monitoring Scope Disabled	Created when the auditing of an ADAM (AD LDS) object is disabled.	Low
ADAM Monitoring Scope Enabled	Created when the auditing of an ADAM (AD LDS) object is enabled.	Low
ADAM Protection Template Added	Created when an ADAM (AD LDS) protection template is added to Change Auditor.	Medium
ADAM Protection Template Changed	Created when an ADAM (AD LDS) protection template is modified.	Medium
ADAM Protection Template Disabled	Created when an ADAM (AD LDS) protection template is disabled.	Medium
ADAM Protection Template Enabled	Created when an ADAM (AD LDS) protection template is enabled.	Medium

Table 1. Change Auditor Internal Auditing events

Event	Description	Severity
ADAM Protection Template Removed	Created when an ADAM (AD LDS) protection template is removed from Change Auditor.	Medium
Administration Account Added to Active Directory Protection Template	Created when an administration account is added to an Active Directory protection template.	Medium
Administration Account Added to Group Policy Protection Template	Created when an administration account is added to a Group Policy protection template.	Medium
Administration Account Removed from Active Directory Protection Template	Created when an administration account is removed from an Active Directory protection template.	Medium
Administration Account Removed from Group Policy Protection Template	Created when an administration account is removed from a Group Policy protection template	Medium
Agent Added to EMC Auditing Template	Created when a Change Auditor agent is added to an EMC Auditing template.	Medium
Agent Added to NetApp Auditing Template	Created when a Change Auditor agent is added to a NetApp Auditing template.	Medium
Agent Added to SharePoint Auditing Template	Created when a Change Auditor agent is added to a SharePoint Auditing template.	Medium
Agent Configuration AD Query Delay Changed	Created when the AD Query auditing delay setting (Discard duplicate queries that occur within *nn* minutes) is changed for an agent configuration definition. (AD Query tab on the Configuration Setup dialog.)	Low
Agent Configuration AD Query Elapsed Changed	Created when the AD Query auditing elapsed setting (Discard queries taking less than *nn* milliseconds) is changed for an agent configuration definition. (AD Query tab on the Configuration Setup dialog.)	Low
Agent Configuration AD Query Results Changed	Created when the AD Query auditing results setting (Discard query results less than *nn* records) is changed for an agent configuration definition. (AD Query tab on the Configuration Setup dialog.)	Low
Agent Configuration Added	Created when a new agent configuration definition is added to Change Auditor.	Low
Agent Configuration Agent Load Threshold Changed	Created when the agent load threshold for an agent configuration definition is modified. (System Settings tab on the Configuration Setup dialog.)	Low
Agent Configuration Assignment Changed	Created when the configuration assignment for a Change Auditor agent is changed.	Low
Agent Configuration Connection Days Changed	Created when the allowed connection days setting is changed for an agent configuration definition. (System Settings tab on the Configuration Setup dialog.)	Low
Agent Configuration Connection From Time Changed	Created when the allowed connection ‘from’ time setting is changed for an agent configuration definition. (System Setting tab on the Configuration Setup dialog.)	Low
Agent Configuration Connection To Time Changed	Created when the allowed connection ‘to’ time setting is changed for an agent configuration definition. (System Settings tab on the Configuration Setup dialog.)	Low
Agent Configuration Exchange Auditing Delay Changed	Created when the Exchange Events setting (Discard duplicates that occur within *nn* seconds) is changed for an agent configuration definition. (Exchange tab on the Configuration Setup dialog.)	Low

Table 1. Change Auditor Internal Auditing events

Event	Description	Severity
Agent Configuration File System Auditing Changed	Created when the file system auditing setting (Audit all configured, including duplicates) is changed for an agent configuration definition. (Exchange tab on the Configuration Setup dialog.)	Low
Agent Configuration File System Auditing Delay Changed	Created when the file system auditing delay setting (Discard duplicates that occur within *nn* seconds) is changed for an agent configuration definition. (Exchange tab on the Configuration Setup dialog.)	Low
Agent Configuration Forwarding Interval Changed	Created when the forwarding interval is changed in a Change Auditor Agent configuration definition. (System Settings tab on the Configuration Setup dialog.)	Low
Agent Configuration Kerberos Ticket Lifetime Changed	Created when an agent's configuration for Kerberos ticket lifetime is changed. (System Settings tab on the Configuration Setup dialog.)	Medium
Agent Configuration Max Events per Connection Changed	Created when the maximum events per connection setting is changed for an agent configuration definition. (System Settings tab on the Configuration Setup dialog.)	Low
Agent Configuration Polling Interval Changed	Created when the polling interval is changed for an agent configuration definition. (System Settings tab on the Configuration Setup dialog.)	Low
Agent Configuration Removed	Created when an agent configuration definition is removed from Change Auditor.	Low
Agent Configuration Renamed	Created when an agent configuration is renamed in Change Auditor.	Low
Agent Configuration Retry Interval Changed	Created when the retry interval is changed for an agent configuration definition. (System Settings on the Configuration Setup dialog.)	Low
Agent configuration service port changed	Created when the communication port between coordinator and agent has changed.	Low
Agent Heartbeat Check Disabled	Created when the **Coordinator should try to restart agent service if an agent goes offline** check box is cleared in the Agent Heartbeat Check pane of the Coordinator Configuration page.	Low
Agent Heartbeat Check Enabled	Created when the **Coordinator should try to restart agent service if an agent goes offline** check box is selected in the Agent Heartbeat Check pane of the Coordinator Configuration page.	Low
Agent Heartbeat Check Minutes Changed	Created when the Agent Heartbeat Check setting (Agent goes offline after being inactive for *nn* minutes) on the Coordinator Configuration page is modified.	Low
Agent Removed from EMC Auditing Template	Created when a Change Auditor agent is removed from an EMC Auditing template.	Medium
Agent Removed from NetApp Auditing Template	Created when a Change Auditor agent is removed from a NetApp Auditing template.	Medium
Agent Removed from SharePoint Auditing Template	Created when a Change Auditor agent is removed from a SharePoint Auditing template.	Medium
Agent Service has more than 100 Events Waiting	Created when the agent has more than 100 events waiting.	Medium
Agent Service has Reached a Critical Load	Created when the agent has reached a critical load and one or more events may have been lost.	High

Table 1. Change Auditor Internal Auditing events

Event	Description	Severity
Agent Service has Returned to Normal Operations	Created when the agent has returned to normal operations.	Low
All specified coordinators that handle purge/archive/report jobs are unavailable	Created when all coordinators specified for purge, archive, and report jobs are inactive. This event is captured when none of the allowed coordinators selected in the Coordinator Configuration page are available. The event is generated every 5 minutes until the issue is fixed.	High
Archive Job Added	Created when an archive job is added.	Medium
Archive Job Completed	Created when an archive job is complete.	Low
Archive Job Changed	Created when an archive job is modified.	Medium
Archive Job Disabled	Created when an archive job is disabled.	Medium
Archive Job Enabled	Created when an archive job is enabled.	Medium
Archive Job Failed	Created when a scheduled archive job fails.	High
Archive Job Removed	Created when an archive job is deleted.	Medium
ArcSight Subscription Added	Created when an ArcSight subscription is added to Change Auditor.	Medium
ArcSight Subscription Removed	Created when an ArcSight subscription is removed from Change Auditor.	Medium
ArcSight Subscription Modified	Created when an ArcSight subscription is modified in Change Auditor.	Medium
Attribute Added to Active Directory Protection	Created when an individual attribute is added to an Active Directory protection template.	Medium
Attribute Added to ADAM Monitoring	Created when an attribute is added to an ADAM (AD LDS) object's auditing scope in Change Auditor.	Low
Attribute Added to ADAM Protection	Created when an attribute is added to an ADAM (AD LDS) protection template.	Medium
Attribute Added to Monitoring	Created when an attribute is added to a directory object's auditing scope in Change Auditor.	Low
Attribute Removed from Active Directory Protection	Created when an attribute is removed from an Active Directory protection template.	Medium
Attribute Removed from ADAM Monitoring	Created when an attribute is removed from an ADAM (AD LDS) object's auditing scope in Change Auditor.	Low
Attribute Removed from ADAM Protection	Created when an attribute is removed from an ADAM (AD LDS) protection template.	Medium
Attribute Removed from Monitoring	Created when an attribute is removed from an object's auditing scope in Change Auditor.	Low
Attribute Severity Changed	Created when the severity for an attribute is changed on the Attribute Auditing page in the Administration Tasks tab.	Low
Audit Event Description Changed	Created when the description is changed for a Change Auditor audited event.	Low
Audit Event Disabled	Created when an event is disabled.	Low
Audit Event Enabled	Created when an event is enabled.	Low
Audit Event Results Changed	Created when the results setting for an audit event is changed on the Audit Events page.	Low
Audit Event Severity Changed	Created when the severity level for a Change Auditor audit event is changed.	Low

Table 1. Change Auditor Internal Auditing events

Event	Description	Severity
Auditing Disabled for EMC Path	Created when auditing of an individual audit path (i.e., file, folder or volume) is disabled in an EMC Auditing template.	Medium
Auditing Disabled for File System Path	Created when auditing of an individual file path is disabled in a File System Auditing template.	Medium
Auditing Disabled for NetApp Path	Created when auditing of an individual audit path (i.e., file, folder or volume) is disabled in a NetApp Auditing template.	Medium
Auditing Disabled for Registry Object	Created when auditing of an individual registry object is disabled in a Registry Auditing template.	Medium
Auditing Disabled for Service	Created when auditing of an individual service is disabled in a Service Auditing template.	Medium
Auditing Disabled for SharePoint Path	Created when auditing of an individual SharePoint path is disabled in a SharePoint Auditing template.	Medium
Auditing Disabled for SQL Instance	Created when auditing of an individual SQL instance is disabled in a SQL Auditing template.	Medium
Auditing Enabled for EMC Path	Created when auditing of an individual audit path (i.e., file, folder or volume) is enabled in an EMC Auditing template.	Medium
Auditing Enabled for File System Path	Created when auditing of an individual file path is enabled in a File System Auditing template.	Medium
Auditing Enabled for NetApp Path	Created when auditing of an individual audit path (i.e., file, folder or volume) is disabled in a NetApp Auditing template.	Medium
Auditing Enabled for Registry Object	Created when auditing of an individual registry object is enabled in a Registry Auditing template.	Medium
Auditing Enabled for Service	Created when auditing of an individual service is enabled in a Service Auditing template.	Medium
Auditing Enabled for SharePoint Path	Created when auditing of an individual SharePoint path is enabled in a SharePoint Auditing template.	Medium
Auditing Enabled for SQL Instance	Created when auditing of an individual SQL instance is enabled in a SQL Auditing template.	Medium
Authentication options changed	Created when the client authentication mode has been changed.	High
Authorized account added to reporting services template	Created when an authorized account is added to a SQL Reporting Services template.	Medium
Authorized account removed from reporting services template	Created when an authorized account is removed from a SQL Reporting Services template.	Medium
Microsoft Entra auditing has resumed	Created when suspended Microsoft Entra auditing resumes.	Medium
Microsoft Entra auditing has suspended	Created when Microsoft Entra auditing is suspended due to a client or server HTTP error.	High
Microsoft Entra audit logs auditing disabled	Created when Microsoft Entra audit log auditing is disabled.	Medium
Microsoft Entra audit logs auditing enabled	Created when Microsoft Entra audit log auditing is enabled.	Medium
Microsoft Entra auditing template added	Created when an Microsoft Entra auditing template is added.	Medium
Microsoft Entra auditing template enabled	Created when an Microsoft Entra auditing template is enabled.	Medium

Table 1. Change Auditor Internal Auditing events

Event	Description	Severity
Microsoft Entra auditing template disabled	Created when an Microsoft Entra auditing template is disabled.	Medium
Microsoft Entra auditing template modified	Created when an Microsoft Entra auditing template is modified.	Medium
Microsoft Entra auditing template removed	Created when an Microsoft Entra auditing template is removed.	Medium
Microsoft Entra sign-ins auditing disabled	Created when Microsoft Entra sign-ins auditing is disabled.	Medium
Microsoft Entra sign-ins auditing enabled	Created when Microsoft Entra sign-ins auditing is enabled.	Medium
Microsoft Entra web application certificate created	Created when a self-signed certificate is created for an Microsoft Entra web application on a Microsoft Entra tenant.	Mediuim
Microsoft Entra web application created	Created when a Microsoft Entra web application is created on an Microsoft Entra tenant. **NOTE:** When you create a Microsoft Entra auditing template, Change Auditor creates a Microsoft Entra application in the default Microsoft Entra tenant. This is required for authentication.	Medium
Microsoft Entra web application and the Change Auditor agent were modified or reset in auditing template	Created when a Microsoft Entra web application and the Change Auditor agent were modified or reset in auditing template	Medium
Microsoft Entra web application modified or reset in auditing template	Created when a Microsoft Entra application or application key is changed in a Microsoft Entra template.	Medium
Change Auditor Agent Restarted	Created when a Change Auditor agent is restarted.	Medium
Change Auditor Agent Set Uninstalled	Created when a Change Auditor agent is set as ‘uninstalled’.	Medium
Change Auditor Agent Started	Created when a Change Auditor agent is started.	Medium
Change Auditor Agent Stopped	Created when a Change Auditor agent is stopped.	Medium
Change Auditor application group added	Created when an application group is added to Change Auditor.	Medium
Change Auditor application group modified	Created when an application group is modified in Change Auditor.	Medium
Change Auditor application group removed	Created when an application group is removed from Change Auditor.	Medium
Change Auditor Coordinator Set Uninstalled	Created when a Change Auditor coordinator is set as ‘uninstalled’.	Medium
Change Auditor hook disabled due to exception	Generated when an agent hook is automatically disabled due to reaching exception limit.	High
Change Auditor PowerShell Client Logon	Created when a user logs on to Change Auditor using a Change Auditor PowerShell command to create a connection.	Low
Change Auditor PowerShell client logon failed	Created when a user fails to log on to Change Auditor using a Change Auditor PowerShell command to create a connection.	Medium
Change Auditor role definition added	Created when a role definition is added to Change Auditor.	Medium
Change Auditor role definition modified	Created when a role definition is modified in Change Auditor.	Medium

Table 1. Change Auditor Internal Auditing events

Event	Description	Severity
Change Auditor role definition removed	Created when a role definition is removed from Change Auditor.	Medium
Change Auditor SDK Client Logon	Created when an application logs on to Change Auditor using the Change Auditor SDK.	Low
Change Auditor task definition added	Created when a task definition is added to Change Auditor.	Medium
Change Auditor task definition modified	Created when a task definition is modified in Change Auditor.	Medium
Change Auditor task definition removed	Created when a task definition is removed from Change Auditor.	Medium
Change Auditor Unknown Client Logon	Created when an unknown client type logs on to Change Auditor using web services.	High
Change Auditor unknown client logon failed	Created when an unknown client type fails to log on to Change Auditor using web services.	Medium
Change Auditor Web Client Logon	Created when a user logs on to the Change Auditor web client.	Low
Change Auditor web client logon failed	Created when a user fails to log on to the Change Auditor web client.	Medium
Change Auditor Windows Client Logon	Created when an user logs on to Change Auditor Windows client.	Low
Change Auditor Windows client logon failed	Created when an user fails to log on to Change Auditor Windows client.	Medium
Client connectivity disconnect option disabled	Created when the Disconnect all clients after 30 minutes of inactivity option is disabled.	Low
Client connectivity disconnect option enabled	Created when the Disconnect all clients after 30 minutes of inactivity option is enabled.	Low
Coordinator added to scheduled task processing	Created when a coordinator is added to scheduled task processing.	Medium
Coordinator removed from scheduled task processing	Created when a coordinator is removed from scheduled task processing.	Medium
Do not enforce protection for GPOADmin working copy option disabled	Created when the "Do not enforce protection for working copy group policies" option is disabled for a Group Policy protection template.	Medium
Do not enforce protection for GPOADmin working copy option enabled	Created when the "Do not enforce protection for working copy group policies" option is enabled for a Group Policy protection template.	Medium
Email Reply To Changed	Created when the Reply To address is changed in the SMTP Configuration pane of the Coordinator Configuration page.	Low
Email Subject Changed	Created when the Email Subject line is changed in the SMTP Configuration pane of the Coordinator Configuration page.	Low
EMC Auditing cepp.conf Changed	Created when the cepp.conf configuration file is changed using the EMC Auditing wizard.	Medium
EMC Auditing Template Added	Created when a new EMC Auditing template is added to Change Auditor.	Medium
EMC Auditing Template Disabled	Created when an EMC Auditing template is disabled.	Medium
EMC Auditing Template Enabled	Created when an EMC Auditing template is enabled.	Medium

Table 1. Change Auditor Internal Auditing events

Event	Description	Severity
EMC Auditing Template Removed	Created when an EMC Auditing template is removed from Change Auditor.	Medium
EMC Path Added to Auditing Template	Created when an audit path (i.e., file, folder or volume) is added to an EMC Auditing template.	Medium
EMC Path Changed in Auditing Template	Created when an audit path (i.e., file, folder or volume) is changed in an EMC Auditing template.	Medium
EMC Path Removed from Auditing Template	Created when an audit path (i.e., file, folder or volume) is removed from an EMC Auditing template.	Medium
Event forwarding has resumed	Created when an event notification sent to the webhook receiver no longer generates a recoverable exception.	Low
Event forwarding subscription disabled due to webhook receiver error	Created when a 401 (unauthorized) or 403 (forbidden) exception on an event or heartbeat notification is received from an event webhook receiver and the subscription is disabled.	High
Event forwarding suspended due to webhook error	Created when an event notification sent to the webhook receiver generates a recoverable exception.	Medium
Event Logging Changed	Created when event logging is modified (enabled or disabled) in Change Auditor.	Low
Event sending to On Demand Audit paused	Created when a user pauses a Change Auditor installation from On Demand Audit.	Medium
Event sending to On Demand Audit resumed	Created when a user resumes a Change Auditor installation from On Demand Audit.	Medium
Exchange Container Added to Protection Template	Created when an Exchange container is added to an Exchange Mailbox Protection template.	Medium
Exchange Container Removed from Protection Template	Created when an Exchange container is removed from an Exchange Mailbox Protection template.	Medium
Exchange Mailbox Added to Monitoring	Created when an Exchange mailbox is added to the Exchange Mailbox Auditing list.	Low
Exchange Mailbox Attribute Changed	Created when the scope of coverage or the Non-owner vs. Non-owner or Owner value is changed for a directory object that is included in the Exchange Mailbox Auditing list.	Low
Exchange Mailbox Disabled	Created when the auditing of a directory object's mailbox is disabled in the Exchange Mailbox Auditing list.	Low
Exchange Mailbox Enabled	Created when the auditing of a directory object's mailbox is enabled in the Exchange Mailbox Auditing list.	Low
Exchange Mailbox Removed from Monitoring	Created when an Exchange mailbox is removed from the Exchange Mailbox Auditing list.	Low
Exchange Password Changed	Created when the password associated with the Exchange host specified in the SMTP Configuration pane of the Coordinator Configuration page is modified.	Low
Exchange Protection Template Added	Created when an Exchange Mailbox Protection template is added to Change Auditor.	Medium
Exchange Protection Template Disabled	Created when an Exchange Mailbox Protection template is disabled.	Medium
Exchange Protection Template Enabled	Created when an Exchange Mailbox Protection template is enabled.	Medium
Exchange Protection Template Removed	Created when an Exchange Mailbox Protection template is removed from Change Auditor.	Medium

Table 1. Change Auditor Internal Auditing events

Event	Description	Severity
Exchange Shared Mailbox Auto Detection Disabled	Created when the automatic detection of shared mailboxes feature is disabled in Change Auditor.	Low
Exchange Shared Mailbox Auto Detection Enabled	Created when the automatic detection of shared mailboxes feature is enabled in Change Auditor.	Low
Exchange User Defined Shared Mailbox Added	Created when a shared mailbox is added to the Exchange Mailbox Auditing list.	Low
Exchange User Defined Shared Mailbox Attribute Changed	Created when the scope of coverage or the Non-owner vs. Non-owner or Owner value is modified for a shared mailbox that is included in the Exchange Mailbox auditing list.	Low
Exchange User Defined Shared Mailbox Disabled	Created when the auditing of a shared mailbox is disabled in the Exchange Mailbox Auditing list.	Low
Exchange User Defined Shared Mailbox Enabled	Created when the auditing of a shared mailbox is enabled in the Exchange Mailbox Auditing list.	Low
Exchange User Defined Shared Mailbox Removed	Created when a shared mailbox is removed from the Exchange Mailbox Auditing list.	Low
Excluded Account Added to Exclusion Accounts List	Created when an excluded account is added to the Change Auditor auditing scope.	Low
Excluded Account Event Class Added to Monitoring	Created when a new event is added to an Excluded Accounts template.	Low
Excluded Account Event Class Removed from Monitoring	Created when an event is removed from an Excluded Accounts template.	Low
Excluded Account Facility Added to Monitoring	Created when a facility (including all of the events in the facility) is added to an Excluded Accounts template.	Low
Excluded Account Facility Removed from Monitoring	Created when a facility (including all of the events in the facility) is removed from an Excluded Accounts template.	Low
Excluded Account Removed from Exclusion Accounts List	Created when an excluded account is removed from the Change Auditor auditing scope.	Low
Excluded Account Template Added	Created when an Excluded Accounts template is added to Change Auditor.	High
Excluded Account Template Added to Agent Configuration	Created when an Excluded Accounts template is added to an agent configuration definition in Change Auditor.	High
Excluded Account Template Removed	Created when an Excluded Accounts template is removed from Change Auditor.	High
Excluded Account Template Removed From Agent Configuration	Created when an Excluded Accounts template is removed from an agent configuration in Change Auditor.	High
File Protection Template Added to Agent Configuration	Created when a File System Protection template is added to an agent configuration definition.	Low
File System Auditing Template Added	Created when a File System Auditing template is added to Change Auditor.	Medium
File System Auditing Template Added to Agent Configuration	Created when a File System Auditing template is added to an agent configuration definition in Change Auditor.	Low
File System Auditing Template Disabled	Created when a File System Auditing template is disabled.	Medium
File System Auditing Template Enabled	Created when a File System Auditing template is enabled.	Medium
File System Auditing Template Removed	Created when a File System Auditing template is removed from Change Auditor.	Medium

Table 1. Change Auditor Internal Auditing events

Event	Description	Severity
File System Auditing Template Removed from Agent Configuration	Created when a File System Auditing template is removed from an agent configuration definition.	Low
File System Path Added to Auditing Template	Created when a file path is added to a File System Auditing template.	Medium
File System Path Added to Protection Template	Created when a file path is added to a File System Protection template.	Medium
File System Path Changed in Auditing Template	Created when a file path is changed in a File System Auditing template.	Medium
File System Path Changed in Protection Template	Created when a file system path is changed in a File System Protection template.	Medium
File System Path Removed from Auditing Template	Created when a file path is removed from a File System Auditing template.	Medium
File System Path Removed from Protection Template	Created when a file path is removed from a File System Protection template.	Medium
File System Protection Template Added	Created when a File System Protection template is added to Change Auditor.	Medium
File System Protection Template Disabled	Created when a File System Protection template is disabled.	Medium
File System Protection Template Enabled	Created when a File System Protection template is enabled.	Medium
File System Protection Template Removed	Created when a File System Protection template is removed from Change Auditor.	Medium
File System Protection Template Removed from Agent Configuration	Created when a File System Protection template is removed from an agent configuration definition.	Low
Group Added for Group Membership Expansion	Created when a group is added to the group membership expansion list on the Coordinator Configuration page in Change Auditor.	Low
Group Added to "Member Of Group" Monitoring	Created when a group is added to the Member of Group Auditing list.	Low
Group Membership Expansion Changed	Created when the group membership expansion option is changed on the Coordinator Configuration page in Change Auditor.	Low
Group Policy Added to Protection Template	Created when a group policy is added to a Group Policy Protection template.	Medium
Group Policy Changed in Protection Template	Created when a group policy is changed in a Group Policy Protection template.	Medium
Group Policy Protection Template Added	Created when a Group Policy Protection template is added to Change Auditor.	Medium
Group Policy Protection Template Disabled	Created when a Group Policy Protection template is disabled.	Medium
Group Policy Protection Template Enabled	Created when a Group Policy Protection template is enabled.	Medium
Group Policy Protection Template Removed	Created when a Group Policy Protection template is removed from Change Auditor.	Medium
Group Policy Removed from Protection Template	Created when a group policy is removed from a Group Policy Protection template.	Medium
Group Removed from Group Membership Expansion	Created when a group is removed from the group membership expansion list on the Coordinator Configuration page in Change Auditor.	Low

Table 1. Change Auditor Internal Auditing events

Event	Description	Severity
Group Removed from "Member Of Group" Monitoring	Created when a group is removed from the Member of Group Auditing list.	Low
IT Security Search Subscription Added	Created when an IT Security Search subscription is added to Change Auditor.	Medium
IT Security Search Subscription Removed	Created when an IT Security Searchsubscription is removed from Change Auditor.	Medium
IT Security Search Subscription Modified	Created when an IT Security Search subscription is modified in Change Auditor.	Medium
Kerberos auditing components failed to load	Created when Kerberos auditing components are not on the domain controller resulting in Kerberos authentication events not being captured.	High
Licensed seats exceeded	Created when an installed Change Auditor licenses is exceeded. The event is generated on coordinator startup and each 24 hours after that when license count is exceeded.	Medium
Microsoft Sentinel subscription added	Created when a Microsoft Sentinel subscription is added to Change Auditor.	Medium
Microsoft Sentinel subscription modified	Created when a Microsoft Sentinel subscription is modified in Change Auditor.	Medium
Microsoft Sentinel subscription removed	Created when a Microsoft Sentinel subscription is removed from Change Auditor.	Medium
Monitoring Point Added	Created when an additional (custom) Active Directory object is added to the Change Auditor auditing scope.	Low
Microsoft 365 Mail Alert Failed	Created when a Microsoft 365 Mail alert notification fails.	Medium
Microsoft 365 Mail alerting Microsoft Entra Directory Name changed	Created when the Microsoft 365 Mail Microsoft Entra Directory Name for mail alerting was changed.	Low
Microsoft 365 Mail alerting enabled	Created Microsoft 365 Mail is enabled for email alerts.	Low
Microsoft 365 Mail alerting disabled	Created Microsoft 365 Mail is disabled for email alerts.	Low
Microsoft 365 Mail alerting web application ID changed	Created when the Microsoft 365 Mail web application ID for mail alerting was changed.	Low
Microsoft 365 Mail alerting web application key changed	Created when the Microsoft 365 Mail web application key for mail alerting was changed.	Low
Microsoft 365 Mail alerting web application successfully created	Created when the Microsoft 365 Mail web application for mail alerting was successfully created on an Microsoft Entra tenant.	Low
Microsoft 365 Mail alerting web application failed to be created	Created when the Microsoft 365 Mail web application for mail alerting failed to be created on the Microsoft Entra tenant.	Low
Monitoring Point Removed	Created when an additional (custom) Active Directory object or object class is removed from the Change Auditor auditing scope.	Low
Monitoring Scope Disabled	Created when the auditing of a directory object is disabled on the Active Directory Auditing page.	Low
Monitoring Scope Enabled	Created when the auditing of a directory object is enabled on the Active Directory Auditing page.	Low
NetApp Auditing Template Added	Created when a new NetApp Auditing template is added to Change Auditor.	Medium
NetApp Auditing Template Disabled	Created when a NetApp Auditing template is disabled.	Medium
NetApp Auditing Template Enabled	Created when a NetApp Auditing template is enabled.	Medium

Table 1. Change Auditor Internal Auditing events

Event	Description	Severity
NetApp Auditing Template Removed	Created when a NetApp Auditing template is removed from Change Auditor.	Medium
NetApp Path Added to Auditing Template	Created when an audit path (i.e., file, folder or volume) is added to a NetApp Auditing template.	Medium
NetApp Path Changed in Auditing Template	Created when an audit path is changed in a NetApp Auditing template.	Medium
NetApp Path Removed from Auditing Template	Created when an audit path (i.e., file, folder or volume) is removed from a NetApp Auditing template.	Medium
Object Added to Active Directory Protection Template	Created when an object is added to an Active Directory Protection template.	Medium
Object Added to ADAM Protection Template	Created when an object is added to an ADAM (AD LDS) Protection template.	Medium
Object Changed in Active Directory Protection Template	Created when an object is modified in an Active Directory Protection template.	Medium
Object Changed in ADAM Protection Template	Created when an object is modified in an ADAM (AD LDS) Protection template.	Medium
Object Removed from Active Directory Protection Template	Created when an object is removed from an Active Directory Protection template.	Medium
Object Removed from ADAM Protection Template	Created when an object is removed from an ADAM (AD LDS) Protection template.	Medium
Microsoft 365 auditing template added	Created when an Microsoft 365 auditing template is added to Change Auditor.	Medium
Microsoft 365 auditing template agent changed	Created when the agent for an existing Microsoft 365 auditing template is changed. The event details include the old and new agent FQDN.	Medium
Microsoft 365 auditing template disabled	Created when an Microsoft 365 auditing template is disabled.	Medium
Microsoft 365 auditing template enabled	Created when an Microsoft 365 auditing template is enabled.	Medium
Microsoft 365 auditing has resumed	Created when suspended Microsoft 365 auditing resumes.	Medium
Microsoft 365 auditing has suspended	Created when Microsoft 365 auditing is suspended due to a client or server HTTP error.	High
Microsoft 365 auditing template removed	Created when an Microsoft 365 auditing template is removed from Change Auditor.	Medium
Microsoft 365 auditing web application certificate changed	Created when the web application certificate is changed for an Microsoft 365 auditing template.	Medium
Microsoft 365 auditing web application changed	Created when the web application is changed for an existing Microsoft 365 template. The event details display the old and new web application ID GUID. **NOTE:** You will also get a Microsoft 365 auditing web application key changed event since the key is a property of the web application.	Medium
Microsoft 365 auditing web application key changed	Created when the web application key is changed for an existing Microsoft 365 template.	Medium
Microsoft 365 Exchange Online “All mailboxes for non-owner events” auditing setting disabled	Created when the “All mailboxes for non-owner events” auditing setting is disabled in an existing Microsoft 365 auditing template.	Medium

Table 1. Change Auditor Internal Auditing events

Event	Description	Severity
Microsoft 365 Exchange Online “All mailboxes for non-owner events” auditing setting enabled	Created when the “All mailboxes for non-owner events” auditing setting is enabled in an existing Microsoft 365 auditing template.	Medium
Microsoft 365 Exchange Online administrative activity auditing setting disabled	Created when the Administrative Activity setting is disabled for an existing Microsoft 365 template.	Medium
Microsoft 365 Exchange Online administrative activity auditing setting enabled	Created when the Administrative Activity setting is enabled for an existing Microsoft 365 template.	Medium
Microsoft 365 Exchange Online auditing disabled	Created when Exchange Online is disabled in an Microsoft 365 auditing template.	Medium
Microsoft 365 Exchange Online auditing enabled	Created when Exchange Online is enabled in an Microsoft 365 auditing template.	Medium
Microsoft 365 Exchange Online mailbox added to auditing template	Created when a mailbox is added to an existing Microsoft 365 auditing template.	Medium
Microsoft 365 Exchange Online mailbox auditing configuration changed by an external application	Created when the following auditing parameters (AuditEnabled, AuditOwner, AuditAdministrator, AuditDelegate) are changed by an application other than Change Auditor. The configuration for the tenant will be reset to settings in the Microsoft 365 auditing template. **NOTE:** The configuration polling runs continuously, with a one hour interval between the end of one pass of all mailboxes and the beginning of the next.	High
Microsoft 365 Exchange Online mailbox auditing configuration failure	Created (at most once every 8 hours) when errors occur trying to reconfigure the auditing properties of an Microsoft 365 Exchange Online mailbox. This typically indicates that the mailbox has been deleted since being added to the auditing template.	High
Microsoft 365 Exchange Online mailbox auditing type changed	Created when the type of activity to audit for a mailbox has changed in a template.	Medium
Microsoft 365 Exchange Online mailbox removed from auditing template	Created when a mailbox is removed from an existing Microsoft 365 auditing template.	Medium
Microsoft 365 OneDrive for Business auditing disabled	Created when OneDrive for Business is disabled in an Microsoft 365 auditing template.	Medium
Microsoft 365 OneDrive for Business auditing enabled	Created when OneDrive for Business is enabled in an Microsoft 365 auditing template.	Medium
Microsoft 365 SharePoint Online auditing disabled	Created when SharePoint Online is disabled in an Microsoft 365 auditing template.	Medium
Microsoft 365 SharePoint Online auditing enabled	Created when SharePoint Online is enabled in an Microsoft 365 auditing template.	Medium
On Demand Audit configuration added	Created when Change Auditor connects to On Demand Audit.	Medium
On Demand Audit configuration removed	Created when a user removes a Change Auditor installation from On Demand Audit or by using the Remove-CAODAConfiguration command.	Medium
On Demand Audit subscription has resumed	Created when event forwarding to On Demand Audit resumes after it has been suspended due to an error.	Medium
On Demand Audit subscription has suspended	Created when event forwarding to On Demand Audit is suspended due to an error.	Medium
Override Account Added to Active Directory Protection Template	Created when an override account is added to an Active Directory Protection template.	Medium

Table 1. Change Auditor Internal Auditing events

Event	Description	Severity
Override Account Added to ADAM Protection Template	Created when an override account is added to an ADAM Protection template.	Medium
Override Account Added to Exchange Protection Template	Created when an override account is added to an Exchange Protection template.	Medium
Override Account Added to File System Protection Template	Created when an override account is added to a File System Protection template.	Medium
Override Account Added to Group Policy Protection Template	Created when an override account is added to a Group Policy Protection template.	Medium
Override Account Removed from Active Directory Protection Template	Created when an override account is removed from an Active Directory Protection template.	Medium
Override Account Removed from ADAM Protection Template	Created when an override account is removed from an ADAM Protection template.	Medium
Override Account Removed from Exchange Protection Template	Created when an override account is removed from an Exchange Protection template.	Medium
Override Account Removed from File System Protection Template	Created when an override account is removed from a File System Protection template.	Medium
Override Account Removed from Group Policy Protection Template	Created when an override account is removed from a Group Policy Protection template.	Medium
Override Accounts Active Directory Protection Template Allow	Created when the override accounts in an Active Directory protection template are set to allow (specifying that accounts are to be excluded from protection).	Medium
Override Accounts Active Directory Protection Template Deny	Created when the override accounts in an Active Directory protection template are set to deny (specifying that accounts are to be included in protection).	Medium
Override Accounts ADAM Protection Template Allow	Created when the override accounts in an ADAM protection template are set to allow (specifying that accounts are to be excluded from protection).	Medium
Override Accounts ADAM Protection Template Deny	Created when the override accounts in an ADAM protection template are set to deny (specifying that accounts are to be included in protection).	Medium
Override Accounts Exchange Protection Template Allow	Created when the override accounts in an Exchange protection template are set to allow (specifying that accounts are to be excluded from protection).	Medium
Override Accounts Exchange Protection Template Deny	Created when the override accounts in an Exchange protection template are set to deny (specifying that accounts are to be included in protection).	Medium
Override Accounts File System Protection Template Allow	Created when the override accounts in a File System protection template are set to allow (specifying that accounts are to be excluded from protection).	Medium
Override Accounts File System Protection Template Deny	Created when the override accounts in a File System protection template are set to deny (specifying that accounts are to be included in protection).	Medium
Override Accounts Group Policy Protection Template Allow	Created when the override accounts in a Group Policy protection template are set to allow (specifying that accounts are to be excluded from protection).	Medium
Override Accounts Group Policy Protection Template Deny	Created when the override accounts in a Group Policy protection template are set to deny (specifying that accounts are to be included in protection).	Medium

Table 1. Change Auditor Internal Auditing events

Event	Description	Severity
Private Report Disabled	Created when reporting is disabled for a private search query (that is, a search created in a user's Private folder) using the Private Alerts and Reports page on the Administration Tasks tab.	Low
Private User Alert Disabled	Created when an alert is disabled for a private search query (that is, a search created in a user's Private folder) using the Private Alerts and Reports page on the Administration Tasks tab.	Low
Private User Search Moved	Created when a a private search is moved using the Private Alerts and Reports page on the Administration Tasks tab.	Low
Private User Search Owner Changed	Created when a private user search is moved to the public area or to the Administrator private folder.	Low
Private User Search Deleted	Created when a a private search is deleted using the Private Alerts and Reports page on the Administration Tasks tab.	Low
Process Added to File System Auditing	Created when a process is added to a File System Auditing template.	Medium
Process Removed from File System Auditing	Created when a process is removed from a File System Auditing template.	Medium
Protection Disabled for Active Directory Object	Created when protection for an Active Directory object is disabled in an Active Directory Protection template.	Medium
Protection Disabled for ADAM Object	Created when protection for an ADAM (AD LDS) object is disabled in an ADAM (AD LDS) Protection template.	Medium
Protection Disabled for File System Path	Created when protection for a file path is disabled in a File System Protection template.	Medium
Protection Enabled for Active Directory Object	Created when protection for an Active Directory object is enabled in an Active Directory Protection template.	Medium
Protection Enabled for ADAM Object	Created when protection for an ADAM (AD LDS) object is enabled in an Active Directory Protection template.	Medium
Protection Enabled for File System Path	Created when protection for a file path is enabled in a File System Protection template.	Medium
Protection for Exchange Container Disabled	Created when protection for an Exchange mailbox is disabled in an Exchange Mailbox Protection template.	Medium
Protection for Exchange Container Enabled	Created when protection for an Exchange mailbox is enabled in an Exchange Mailbox Protection template.	Medium
Protection for Group Policy Disabled	Created when protection for a group policy object is disabled in a Group Policy Protection template.	Medium
Protection for Group Policy Enabled	Created when protection for a group policy object is enabled in a Group Policy Protection template.	Medium
Public Report Disabled	Created when reporting is disabled for a shared search query (that is, a search in a Shared folder).	Low
Public Report Enabled	Created when a reporting is enabled for a shared search query (that is, a search in a Shared folder).	Low
Public User Alert Changed	Created when an alert is changed in Change Auditor for a shared search query (that is, a search in a Shared folder).	Low
Public User Alert Disabled	Created when an alert is disabled in Change Auditor for a shared search query (that is, a search in a Shared folder).	Low

Table 1. Change Auditor Internal Auditing events

Event	Description	Severity
Public User Alert Enabled	Created when an alert is enabled in Change Auditor for a shared search query (that is, a search in a Shared folder).	Low
Public User Search Created	Created when a public user search is created in Change Auditor.	Low
Public User Search Deleted	Created when a public user search is deleted from Change Auditor.	Low
Public User Search Modified	Created when a public user search is modified in Change Auditor.	Low
Purge Job Added	Created when a scheduled purge job is added.	Medium
Purge Job Changed	Created when a scheduled purge job is modified.	Medium
Purge Job Disabled	Created when a scheduled purge job is disabled.	Medium
Purge Job Enabled	Created when a scheduled purge job is enabled.	Medium
Purge Job Removed	Created when a scheduled purge job is deleted.	Medium
Purge and Archive Job Added	Created when a scheduled purge and archive job is added.	Medium
Purge and Archive Job Changed	Created when a scheduled purge and archive job is modified.	Medium
Purge and Archive Job Completed	Created when a scheduled purge and archive job is completed.	Low
Purge and Archive Job Disabled	Created when a scheduled purge and archive job is disabled.	Medium
Purge and Archive Job Enabled	Created when a scheduled purge and archive job is enabled.	Medium
Purge and Archive Job Failed	Created when a scheduled purge and archive job fails.	High
Purge and Archive Job Removed	Created when a scheduled purge and archive job is deleted from the Purge Jobs page on the Administration Tasks tab.	Medium
Purge Job Completed	Created when a scheduled purge job is completed.	Low
Purge Job Failed	Created when a scheduled purge job fails.	High
QRadar Subscription Added	Created when a QRadar subscription is added to Change Auditor.	Medium
QRadar Subscription Removed	Created when a QRadar subscription is removed from Change Auditor.	Medium
QRadar Subscription Modified	Created when a QRadar subscription is modified in Change Auditor.	Medium
Refresh Frequency for Group Membership Changed	Created when the **Refresh Group Membership Every *nnn* Minutes** setting is changed on the Coordinator Configuration page in Change Auditor.	Low
Refresh Frequency for the List of Expanded Groups Changed	Created when the **Refresh the List of Expanded Groups Every *nnn* Minutes** setting is changed on the Coordinator Configuration page in Change Auditor.	Low
Registry Auditing Template Added	Created when a Registry Auditing template is added to Change Auditor.	Medium
Registry Auditing Template Added to Agent Configuration	Created when a Registry Auditing template is added to an agent configuration definition.	Low
Registry Auditing Template Disabled	Created when a Registry Auditing template is disabled.	Medium
Registry Auditing Template Enabled	Created when a Registry Auditing template is enabled.	Medium

Table 1. Change Auditor Internal Auditing events

Event	Description	Severity
Registry Auditing Template Removed	Created when a Registry Auditing template is removed from Change Auditor.	Medium
Registry Auditing Template Removed from Agent Configuration	Created when a Registry Auditing template is removed from an agent configuration definition.	Low
Registry Object Added to Auditing Template	Created when a registry object is added to a Registry Auditing template.	Medium
Registry Object Changed in Auditing Template	Created when a registry object is changed in a Registry Auditing template.	Medium
Registry Object Removed from Auditing Template	Created when a registry object is removed from a Registry Auditing template.	Medium
Report Layout Added	Created when a report layout is added to the Report Layouts page on the Administration Tasks tab.	Medium
Report Layout Changed	Created when a report layout is modified.	Medium
Report Layout Removed	Created when a report layout is deleted from the Report Layouts page on the Administration Tasks tab.	Medium
Scheduled task processing assignment changed	Created when a scheduled task processing assignment has changed.	Medium
Scheduled task processing setting changed	Created when a scheduled task processing setting has changed.	Medium
Scheduled report failed	Created when a scheduled report fails. (For example, issues with Exchange or invalid search settings.)	Medium
SDK Agent Added	Created when an agent (machine where the audit event occurred) is added using the software development kit.	Medium
SDK Event Class Added	Created when a new user-defined event class (type of audit event) is added to Change Auditor using the software development kit.	Medium
SDK Event Class Modified	Created when a user-defined event class is modified using the software development kit.	Medium
SDK Event Class Removed	Created when a user-defined event class is removed from Change Auditor using the software development kit.	Medium
SDK Facility Added	Created when a new user-defined facility (category of an event class) is added to Change Auditor using the software development kit.	Medium
SDK Facility Modified	Created when a user-defined facility is modified (e.g., new events are added or removed) using the software development kit.	Medium
SDK Facility Removed	Created when a user-defined facility is removed from Change Auditor using the software development kit.	Medium
SDK Machine Added	Created when a workgroup server (machine where the audit event occurred) is added using the software development kit. (Used in ADAM (AD LDS) configurations only.)	Medium
Service Added to Auditing Template	Created when a service is added to a Service Auditing template.	Medium
Service Auditing Template Added	Created when a Service Auditing template is added to Change Auditor.	Medium
Service Auditing Template Added to Agent Configuration	Created when a Service Auditing template is added to an agent configuration definition.	Low
Service Auditing Template Changed	Created when a Service Auditing template is modified.	Medium

Table 1. Change Auditor Internal Auditing events

Event	Description	Severity
Service Auditing Template Disabled	Created when a Service Auditing template is disabled.	Medium
Service Auditing Template Enabled	Created when a Service Auditing template is enabled.	Medium
Service Auditing Template Removed	Created when a Service Auditing template is removed from Change Auditor.	Medium
Service Auditing Template Removed from Agent Configuration	Created when a Service Auditing template is removed from an agent configuration definition.	Low
Service Removed from Auditing Template	Created when a service is removed from a Service Auditing template.	Medium
SharePoint Auditing Template Added	Created when a SharePoint Auditing template is added in Change Auditor.	Medium
SharePoint Auditing Template Disabled	Created when a SharePoint Auditing template is disabled.	Medium
SharePoint Auditing Template Enabled	Created when a previously disabled SharePoint Auditing template is enabled.	Medium
SharePoint Auditing Template Removed	Created when a SharePoint Auditing template is removed from Change Auditor.	Medium
SharePoint Event Added	Created when a SharePoint event is added to a SharePoint Auditing template.	Medium
SharePoint Event Removed	Created when a SharePoint event is removed from a SharePoint Auditing template.	Medium
SharePoint Facility Added	Created when a SharePoint facility is added to a SharePoint Auditing template	Medium
SharePoint Facility Removed	Created when a SharePoint facility is removed from a SharePoint Auditing template.	Medium
SharePoint Path Added to Auditing Template	Created when a SharePoint path is added to a SharePoint Auditing template.	Medium
SharePoint Path Changed in Auditing Template	Created when a SharePoint path is modified in a SharePoint Auditing template.	Medium
SharePoint Path Removed From Auditing Template	Created when a SharePoint path is removed from a SharePoint Auditing template.	Medium
SMTP Alert Failed	Created when an SMTP alert notification fails.	Medium
SMTP Alerting Disabled	Created when the **Enable SMTP for Alerts and Reporting** check box is cleared in the SMTP Configuration pane of the Coordinator Configuration page.	Low
SMTP Alerting Email Format Changed	The email format (Plain Text or HTML) used for SMTP notifications is changed in the SMTP Configuration pane of the Coordinator Configuration page.	Low
SMTP Alerting Enabled	Created when the **Enable SMTP for Alerts and Reporting** check box is selected in the SMTP Configuration pane of the Coordinator Configuration page.	Low
Email Alerting From Address Changed	Created when the From Address used for email notifications is changed in the Coordinator Configuration page.	Low
SMTP Alerting Server Authentication Disabled	Created when the **My Server Requires Authentication** check box is cleared in the SMTP Configuration pane of the Coordinator Configuration page.	Low

Table 1. Change Auditor Internal Auditing events

Event	Description	Severity
SMTP Alerting Server Authentication Enabled	Created when the **My Server Requires Authentication** check box is selected in the SMTP Configuration pane of the Coordinator Configuration page.	Low
SMTP Alerting Server Changed	Created when the mail server used for SMTP alerting and reporting is changed in the SMTP Configuration pane of the Coordinator Configuration page.	Low
SMTP Alerting Server Password Changed	Created when the password associated with the mail server specified in the SMTP Configuration pane of the Coordinator Configuration page is modified.	Low
SMTP Alerting Server Username Changed	Created when the account name associated with the mail server specified in the SMTP Configuration pane of the Coordinator Configuration page is modified.	Low
SMTP Lookup Exchange Account Changed	Created when the account name associated with the Exchange host specified in the SMTP Configuration pane of the Coordinator Configuration page is modified.	Low
SMTP Lookup Exchange Authorization Disabled	Created when the **My Host Requires Authentication** check box is cleared in the SMTP Configuration pane of the Coordinator Configuration page.	Low
SMTP Lookup Exchange Authorization Enabled	Created when the **My Host Requires Authentication** check box is selected in the SMTP Configuration pane of the Coordinator Configuration page.	Low
SMTP Lookup Exchange Email Changed	Created when the email address associated with the Exchange host in the SMTP Configuration pane of the Coordinator Configuration page is modified.	Low
SMTP Lookup Exchange Host Changed	Created when the Exchange host in the SMTP Configuration pane of the Coordinator Configuration page is modified	Low
SMTP Lookup Exchange Password Changed	Created when the password associated with the Exchange host specified in the SMTP Configuration pane of the Coordinator Configuration page is modified.	Low
SMTP Lookup Exchange Version Changed	Created when the version number associated with the Exchange host in the SMTP Configuration pane of the Coordinator Configuration page is modified.	Low
SMTP Ssl Disabled	Created when the **Enable SSL** check box is cleared in the SMTP Configuration pane of the Coordinator Configuration page.	Low
SMTP Ssl Enabled	Created when the **Enable SSL** check box is selected in the SMTP Configuration pane of the Coordinator Configuration page.	Low
Splunk subscription added	Created when a Splunk subscription is added to Change Auditor.	Medium
Splunk subscription modified	Created when a Splunk subscription is changed in Change Auditor.	Medium
Splunk subscription removed	Created when a Splunk subscription is removed from Change Auditor.	Medium
SQL Auditing Template Added	Created when a new SQL Auditing template is added to Change Auditor.	Medium
SQL Auditing Template Added to Agent Configuration	Created when a SQL Auditing template is added to an agent configuration definition.	Low
SQL Auditing Template Disabled	Created when a SQL Auditing template is disabled.	Medium
SQL Auditing Template Enabled	Created when a SQL Auditing template is enabled.	Medium

Table 1. Change Auditor Internal Auditing events

Event	Description	Severity
SQL Auditing Template Removed	Created when a SQL Auditing template is removed from Change Auditor.	Medium
SQL Auditing Template Removed from Agent Configuration	Created when a SQL Auditing template is removed from an agent configuration definition.	Low
SQL Data Level Auditing Template Added	Created when a new SQL Data Level Auditing template is created.	Medium
SQL Data Level Auditing Template Deleted	Created when a SQL Data Level Auditing template is removed.	Medium
SQL Data Level Auditing Template Enabled	Created when a SQL Data Level Auditing template is enabled.	Medium
SQL Data Level Auditing Template Disabled	Created when a SQL Data Level Auditing template is disabled.	Medium
SQL Data Level Auditing Template Modified	Created when a SQL Data Level Auditing template is modified.	Medium
SQL Event Added	Created when a SQL event is added to a SQL Auditing template.	Medium
SQL Event Removed	Created when a SQL event is removed from a SQL Auditing template.	Medium
SQL Extended Events auditing template added	Created when an SQL Extended Events auditing template is added.	Medium
SQL Extended Events auditing template deleted	Created when an SQL Extended Events auditing template is removed.	Medium
SQL Facility Added	Created when a SQL facility is added to a SQL Auditing template.	Medium
SQL Facility Removed	Created when a SQL facility is removed from a SQL Auditing template.	Medium
SQL Filter Added	Created when a SQL filter is added to a SQL Auditing template.	Medium
SQL Filter Removed	Created when a SQL filter is removed from a SQL Auditing template.	Medium
SQL Instance Added	Created when a SQL instance is added to a SQL Auditing template.	Medium
SQL Instance Removed	Created when a SQL instance is removed from a SQL Auditing template.	Medium
SQL Reporting Services template added	Created when a SQL Reporting Services template is added to Change Auditor.	Medium
SQL Reporting Services template disabled	Created when a SQL Reporting Services template is disabled.	Medium
SQL Reporting Services template enabled	Created when a SQL Reporting Services template is enabled	Medium
SQL Reporting Services template removed	Created when a SQL Reporting Services template is removed from Change Auditor.	Medium
SRS URL added to reporting services template	Created when an SRS URL is added to a SQL Reporting Services template.	Medium
SRS URL attribute changed	Created when an SRS URL attribute is modified in a SQL Reporting Services template.	Low
Syslog subscription added	Created when a syslog subscription is added through the client or the new-CASyslogEventSubscription command.	Medium

Table 1. Change Auditor Internal Auditing events

Event	Description	Severity
Syslog subscription modified	Created when a syslog subscription is changed through the client or the set-CASyslogEventSubscription command.	Medium
Syslog subscription removed	Created when a syslog subscription is removed through the client or the remove-CASyslogEventSubscription command.	Medium
The Number of Groups to Expand per Cycle Changed	Created when the **Number of Groups to Expand Every 5-Minute Cycle** setting is changed on the Coordinator Configuration page in Change Auditor.	Low

Custom Registry Monitoring

Table 2. Custom Registry Monitoring events

Event	Description	Severity
Binary Registry Value Added	Created when a binary value is added to a registry key.	Medium
Binary Registry Value Changed	Created when a binary value is changed in a registry key.	Medium
Binary Registry Value Deleted	Created when a binary value is deleted from a registry key.	Medium
Numeric Registry Value Added	Created when a numeric value is added to a registry key.	Medium
Numeric Registry Value Changed	Created when a numeric value is changed in a registry key.	Medium
Numeric Registry Value Deleted	Created when a numeric value is deleted from a registry key.	Medium
Registry Key Added	Created when a registry key is added.	Medium
Registry Key DACL Changed	Created when the DACL for a registry key is modified. **NOTE:** This event is only captured for Windows Server 2008 (and higher).	Medium
Registry Key Deleted	Created when a registry key is deleted.	Medium
Registry Key Owner Changed	Created when the owner of a registry key is modified. **NOTE:** This event is only captured for Windows Server 2008 (and higher).	Medium
Registry Key SACL Changed	Created when the SACL for a registry key is modified. **NOTE:** This event is only captured for Windows Server 2008 (and higher).	Medium
String Registry Value Added	Created when a string value is added to the registry key.	Medium
String Registry Value Changed	Created when a string value is changed in the registry key.	Medium
String Registry Value Deleted	Created when a string value is deleted from the registry key.	Medium

Fault Tolerance

Table 3. Fault Tolerance events

Event	Description	Severity
Change Auditor Agent Connected	Created when a Change Auditor agent connects to the Change Auditor coordinator service.	Low
Change Auditor Agent Disconnected	Created when a Change Auditor agent disconnects from the Change Auditor coordinator service.	Medium
Change Auditor Agent Lost Heartbeat	Created when a Change Auditor agent has lost heartbeat and is considered inactive.	Low
Change Auditor Agent Restarted	Created when a Change Auditor agent is restarted.	Low
Change Auditor Agent Uninstalled	Created when a Change Auditor agent is uninstalled.	Low
Topology Server Added	Created when a Change Auditor coordinator is notified that a new server has been added to the topology.	Low
Topology Server Removed	Created when a Change Auditor coordinator is notified that a server has been removed from the topology.	Low
Topology Workstation Added	Created when a Change Auditor coordinator is notified that a workstation has been added to the topology.	Low

Local Group Monitoring

Table 4. Local Group Monitoring events

Event	Description	Severity
Local Group Added	Created when a local group is added to a member server using the MMC Local Users and Groups snap-in or the NET LOCALGROUP command line.	Medium
Local Group Removed	Created when a local group is removed from a member server using the MMC Local Users and Groups snap-in or the NET LOCALGROUP command line.	Medium
Local Group Renamed	Created when a local group is renamed on a member server using the MMC Local Users and Groups snap-in.	Medium
Member Added to Local Group	Created when group or user members are added to a local group on a member server using the MMC Local Users and Groups snap-in or the NET LOCALGROUP command line.	Medium
Member Removed from Local Group	Created when group or user members are removed from a local group on a member server using the MMC Local Users and Groups snap-in or the NET LOCALGROUP command line.	Medium

Local User Monitoring

Table 5. Local User Monitoring events

Event	Description	Severity
Account Disabled for Local User	Created when a local user account is disabled using the MMC Local Users and Computers snap-in or the NET USER/ACTIVE command line.	Medium
Account Enabled for Local User	Created when a local user account is enabled using the MMC Local Users and Computers snap-in or the NET USER/ACTIVE command line.	Medium
Account Expiration Changed for Local User	Created when the expiration date/time is changed for a local user account.	Medium
Active Session Limit Changed for Local User	Created when the Active session limit timeout value is changed in the Terminal Services Session settings for a user account.	Medium
Allow Reconnection Option Changed for Local User	Created when the Allow reconnection option is changed in the Terminal Services Environment for a user account.	Medium
Can't Change Password Changed for Local User	Created when the User can’t change password option is enabled or disabled for a local user account.	Medium
Connect Client Drives at Logon Changed for Local User	Created when the Connect client drives at logon option is changed in the Terminal Services Environment for a user account.	Medium
Connect Client Printers at Logon Changed for Local User	Created when the Connect client printers at logon option is changed in the Terminal Services Environment for a user account.	Medium
Default to Main Client Printer Changed for Local User	Created when the Default to main client printer option is changed in the Terminal Services Environment for a user account.	Medium
Deny This User Terminal Services Permission Changed for Local User	Created when the Deny this user permission to log on to any Terminal Server option is changed in the Terminal Services Profile settings for a local user account on a member server.	Medium
Dial-in Callback Number Changed for Local User	Created when the Callback number is changed in the Remote Access Dial-in and VPN settings for a local user account on a member server.	Medium
Dial-in Callback Options Changed for Local User	Created when the Callback options setting is changed in the Remote Access Dial-in and VPN settings for a local user account on a member server.	Medium
Dial-in Static IP Address Changed for Local User	Created when the Assign a Static IP Address setting is changed in the Remote Access Dial-in and VPN settings for a local user account on a member server.	Medium
Dial-in Static Routes Changed for Local User	Created when the Apply Static Routes setting is changed in the Remote Access Dial-in and VPN settings for a local user account on a member server.	Medium
Dial-in Verify Caller-ID Changed for Local User	Created when the caller-ID setting is changed in the Remote Access Dial-in and VPN settings for a local user account on a member server.	Medium
Disconnected Session Timeout Changed for Local User	Created when the End a disconnected session timeout value is changed in the Terminal Services Session settings for a user account.	Medium

Table 5. Local User Monitoring events

Event	Description	Severity
Enable Remote Control Changed for Local User	Created when the Enable remote control option is changed in the Terminal Services Remote Control settings for a user account.	Medium
Home Folder Mapped Drive Changed for Local User	Created when the home folder remote mapped drive for a user account is changed using the MMC Local Users and Groups snap-in.	Medium
Home Folder Path Changed for Local User	Created when the home folder local or remote path for a user account is changed using the MMC Local Users and Groups snap-in or NET USER/HOMEDIR command line.	Medium
Idle Session Limit Changed for Local Users	Created when the Idle session limit timeout value is changed in the Terminal Services Environment for a user account.	Medium
Local User Account Locked	Created when the number of successive failed logon attempts using a local user account on a member server exceeds the threshold set for the account lockout policy on that server.	Medium
Local User Account Unlocked	Created when a local user account is unlocked by an administrator. The account can be unlocked using the MMC Local Users and Computers snap-in.	Medium
Local User Added	Created when a local user is added to a member server using the MMC Local Users and Groups snap-in or the NET USER command line.	Medium
Local User badPwdCount Changed	Created when a logon attempt using a local user account on a member server fails due to an incorrect password.	Medium
Local User Logged On	Created when a user logs on using a local user account on a member server.	Medium
Local User Removed	Created when a local user is removed from a member server using the MMC Local Users and Groups snap-in or the NET USER command line.	Medium
Local User Renamed	Created when a local user is renamed on a member server using the MMC Local Users and Groups snap-in.	Medium
Logon Program Filename Changed for Local User	Created when the starting program filename is changed in the Terminal Services Environment for a user account.	Medium
Logon Program Folder Changed for Local User	Created when the logon program folder is changed in the Terminal Services Environment for a user account.	Medium
Logon Script Changed for Local User	Created when the logon script for a local user account is changed using the MMC Local Users and Groups snap-in or NET USER/SCRIPTPATH command line.	Medium
Must Change Password At Next Logon Changed for Local User	Created when the User must change password at next logon option is enabled or disabled for a local user account.	Medium
Password Changed for Local User	Created when the password for a local user account is changed.	Medium
Password Never Expires Changed for Local User	Created when the Password Never Expires option is enabled or disabled for a local user account.	Medium
Password Required Changed for Local User	Created when the Password Required option is enabled or disabled for a local user account.	Medium

Table 5. Local User Monitoring events

Event	Description	Severity
Profile Path Changed for Local User	Created when the path profile for a local user account is changed using the MMC Local Users and Groups snap-in or NET USER/PROFILEPATH command line.	Medium
Remote Access Permission Changed for Local User	Created when the Remote access permission (Dial-in or VPN) option is changed in the Remote Access Dial-in and VPN settings for a local user account on a member server.	Medium
Remote Control Level of Control Changed for Local User	Created when the Level of control option is changed in the Terminal Services Remote Control settings for a user account.	Medium
Remote Control Require User's Permission Changed for Local User	Created when the Require User's Permission option is changed in the Terminal Services Remote Control settings for a user account.	Medium
Session Limit Action Changed for Local User	Created when the When session limit is reached or connection is broken option is changed in the Terminal Services Environment for a user account.	Medium
Start the Following Program at Logon Changed for Local User	Created when the Start following programs at logon option is changed in the Terminal Services Environment for a user account.	Medium
Terminal Services Home Folder Mapped Drive Changed for Local User	Created when the Terminal Services home folder remote mapped drive is changed in the Terminal Services Profile settings for a local user account on a member server.	Medium
Terminal Services Home Folder Path Changed for Local User	Created when the Terminal Services home folder local or remote path is changed in the Terminal Services Profile settings for a local user account on a member server.	Medium
Terminal Services Profile Path Changed for Local User	Created when the profile path is changed in the Terminal Services Profile settings for a local user account on a member server.	Medium

Service Monitoring

Table 6. Service Monitoring events

Event	Description	Severity
Service Account Changed	Created when a service account is changed.	High
Service Dependencies Changed	Created when a dependency for a service is changed.	Medium
Service Paused	Created when a service is paused.	Medium
Service Recovery Actions Changed	Created when the recovery actions for a service is changed.	Medium
Service Resumed	Created when a service is resumed after it has been paused.	Medium
Service Start Type Changed	Created when the start type of a service is changed.	Medium
Service Started	Created when a service is started.	Medium
Service Stopped	Created when a service is stopped.	Medium

System Events

Table 7. System events

Event	Description	Severity
Application Event Log Cleared	Created whenever the Application Event log is cleared.	High
Application Event Log Rolled Over	Created when the application event log is rolled over. (Disabled by default)	Medium
Automatic Updates Day Setting Changed	Created when the Automatic Updates day setting is changed.	Medium
Automatic Updates Option Changed	Created when the Automatic Updates option is changed.	Medium
Automatic Updates Time Setting Changed	Created when the Automatic Updates time setting is changed.	Medium
Crash on Audit Fail Policy Changed	Created when the Crash on Audit Fail policy is changed.	Low
Disk Size Changed	Created when the size of the disk that stores the SySvol and DSA Working Directory on the domain controller has been changed. **NOTE:** This event is only generated when the agent is restarted on the domain controller.	Low
Global Catalog Lookup for Logon Requirement Changed	Created when the GC logon lookup requirement is changed.	Medium
Memory Amount Changed	Created when the physical memory of the DC is changed.	Low
Remote Assistance Invitation Time Unit Changed	Created when the Remote Assistance Invitation Time Unit setting has changed.	Medium
Remote Assistance Invitation Time Value Changed	Created when the Remote Assistance Invitation Time Value setting has changed.	Medium
Remote Assistance Option Changed	Created when the Remote Assistance option setting has changed.	Medium
Remote Assistance Remote Control Option Changed	Created when the Remote Assistance Remote Control option setting has changed.	Medium
Remote Desktop Create Invitations for Only Windows Vista or Later Option Changed	Created when the Remote Desktop Create Invitations for Only Windows Vista or Later option setting has changed.	Medium
Remote Desktop Option Changed	Created when the Remote Desktop option setting has changed.	Medium
Security Audit Log Rolled Over	Created when the security audit log is rolled over. (Disabled by default)	Medium
Security Event Log Cleared	Created when the security event log is cleared (event 517 is encountered).	High
System Event Log Cleared	Created when the system log is cleared using the Clear All Events command in the Event Viewer.	High
System Event Log Rolled Over	Created when the system event log is rolled over. (Disabled by default)	Medium

3

Log Events

When event logging for Change Auditor is enabled, internal Change Auditor events will be written to a Windows event log, named Change Auditor Coordinator Service event log. In addition, when event logging for Registry, Service and/or Local Account is enabled in Change Auditor, related events will be written to the Change Auditor Service event log. These log events can then be gathered by InTrust 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.

The tables in this chapter list the log events captured by the different event logs when the corresponding event logging is enabled. They are listed in numeric order by event ID based on the event log to which they are recorded:

- Change Auditor Coordinator Service event log
- Change Auditor Service event log

Change Auditor Coordinator Service event log

The following internal Change Auditor events are recorded to the Change Auditor Coordinator Service event log when Change Auditor event logging is enabled.

Table 8. Change Auditor Coordinator Service event log events

Event ID	Description
101	Agent configuration assignment changed
102	Agent configuration added
103	Agent configuration removed
104	Agent configuration forwarding interval changed
105	Agent configuration retry interval changed
106	Agent configuration polling interval changed
107	Agent configuration max events per connection changed
108	Agent configuration connection days changed
109	Agent configuration connection from time changed
110	File system auditing template added to agent configuration
111	File system auditing template removed from agent configuration
112	Agent configuration renamed
113	Registry auditing template added to agent configuration
114	Registry auditing template removed from agent configuration
115	Excluded account template added to agent configuration
116	Excluded account template removed from agent configuration
127	Service auditing template added to agent configuration

Table 8. Change Auditor Coordinator Service event log events

Event ID	Description
128	Service auditing template removed from agent configuration
129	File system protection template added to agent configuration
130	File system protection template removed from agent configuration
131	Agent configuration file system auditing changed
132	Agent configuration file system auditing delay changed
133	Agent configuration connection to time changed
134	SQL auditing template added to agent configuration
135	SQL auditing template removed from agent configuration
136	Agent configuration AD Query auditing results changed
137	Agent configuration AD Query auditing elapsed changed
138	Agent configuration AD Query auditing delay changed
139	Event logging changed
140	Alert History purge changed
141	Agent configuration exchange auditing delay changed
143	Agent configuration agent load threshold changed
154	Communications port between coordinator and agent has changed
155	A Microsoft Entra web application has been created on Microsoft Entra tenant
156	The Microsoft Entra web application in auditing template was modified
157	The Microsoft Entra web applicationand the Change Auditor agent used in auditing template were modified or reset
201	Audit event severity changed
202	Audit event description changed
203	Audit event enabled
204	Audit event disabled
205	Audit event results changed
301	Monitoring point added
302	Monitoring point removed
303	Attribute added to monitoring
304	Attribute removed from monitoring
305	Group added to ‘Member of Group’ monitoring
306	Group removed from ‘Member of Group’ monitoring
307	Attribute severity changed
308	Monitoring scope enabled
309	Monitoring scope disabled
310	Active Directory protection template added
311	Active Directory protection template removed
312	Active Directory protection template enabled
313	Active Directory protection template disabled
314	Object added to Active Directory protection template
315	Object removed from Active Directory protection template
316	Protection enabled for Active Directory object
317	Protection disabled for Active Directory object
318	Override account added to Active Directory protection template

Table 8. Change Auditor Coordinator Service event log events

Event ID	Description
319	Override account removed from Active Directory protection template
320	Attribute added to Active Directory protection
321	Attribute removed from Active Directory protection
322	Object changed in Active Directory protection template
323	Active Directory protection template changed
324	Administration account added to Active Directory protection template
325	Administration account removed from Active Directory protection template
326	Administration account added to Group Policy protection template
327	Administration account removed from Group Policy protection template
401	ADAM monitoring point added
402	ADAM monitoring point removed
403	Attribute added to ADAM monitoring
404	Attribute removed from ADAM monitoring
405	ADAM attribute severity changed
406	ADAM monitoring scope enabled
407	ADAM monitoring scope disabled
408	ADAM protection template added
409	ADAM protection template removed
410	ADAM protection template enabled
411	ADAM protection template disabled
412	Object added to ADAM protection template
413	Object removed from ADAM protection template
414	Protection enabled for ADAM object
415	Protection disabled for ADAM object
416	Override account added to ADAM protection template
417	Override account removed from ADAM protection template
418	Attribute added to ADAM protection
419	Attribute removed from ADAM protection
420	Object changed in ADAM protection template
421	ADAM protection template changed
422	Override accounts ADAM protection template Allow
423	Override accounts ADAM protection template Deny
501	SMTP alerting enabled
502	SMTP alerting disabled
503	SMTP alerting server changed
504	SMTP alerting from address changed
505	SMTP alerting email format changed
506	SMTP alerting server authentication enabled
507	SMTP alerting server authentication disabled
508	SMTP alerting server username changed
509	SMTP alerting server password changed
510	Email Subject changed

Table 8. Change Auditor Coordinator Service event log events

Event ID	Description
511	Email Reply To changed
512	Group membership expansion changed
513	Refresh frequency for group membership changed
514	Refresh frequency for the list of expanded groups changed
515	The number of groups to expand per cycle changed
516	Group added for group membership expansion
517	Group removed form group membership expansion
518	Agent Heartbeat Check Minutes changed
519	Agent Heartbeat Check enabled
520	Agent Heartbeat Check disabled
521	Smtp Ssl enabled
522	Smtp Ssl disabled
523	Exchange Host changed
524	Exchange Email changed
525	Exchange Authorization enabled
526	Exchange Account changed
527	Exchange Password changed
528	Exchange Authorization disabled
529	Exchange Version changed
604	Public user alert enabled
605	Public user alert disabled
606	Public user alert changed
607	Public user search changed
608	Public user search deleted
609	Public user search modified
610	Public report enabled
611	Public report disabled
613	Private user alert disabled
615	Private report disabled
640	Public user search moved
641	Public user search folder deleted
642	Public user search folder moved
643	Public user alert deleted
644	Public user alert moved
645	Public user search folder renamed
646	Public user alert created
701	File system auditing template added
702	File system auditing template removed
703	File system path changed in auditing template
704	File system path added to auditing template
705	File system path removed from auditing template
706	Process added to file system auditing

Table 8. Change Auditor Coordinator Service event log events

Event ID	Description
707	Process removed from file system auditing
709	File system auditing template enabled
710	File system auditing template disabled
711	Auditing enabled for file system path
712	Auditing disabled for file system path
713	File system protection template added
714	File system protection template removed
715	File system path changed in protection template
716	File system path added to protection template
717	File system path removed from protection template
718	Protection enabled for file system path
719	Protection disabled for file system path
720	File system protection template enabled
721	File system protection template disabled
722	Override account added to file system protection template
723	Override account removed from file system protection template
724	Override accounts file system protection template Allow
725	Override accounts file system protection template Deny
726	Override accounts Active Directory protection template Allow
727	Override accounts Active Directory protection template Deny
801	Registry auditing template added
802	Registry auditing template removed
803	Registry object changed in auditing template
804	Registry object added to auditing template
805	Registry object removed from auditing template
806	Auditing enabled for registry object
807	Auditing disabled for registry object
808	Registry auditing template enabled
809	Registry auditing template disabled
901	Group Policy protection template added
902	Group Policy protection template removed
903	Group Policy protection template enabled
904	Group Policy protection template disabled
905	Group Policy added to protection template
906	Group Policy removed from protection template
907	Protection for Group Policy enabled
908	Protection form Group Policy disabled
909	Override account added to Group Policy protection template
910	Override account removed from Group Policy protection template
911	Group Policy changed in protection template
912	Override accounts Group Policy protection template Allow
913	Override accounts Group Policy protection template Deny

Table 8. Change Auditor Coordinator Service event log events

Event ID	Description
1001	Excluded account template added
1002	Excluded account template removed
1003	Excluded account added to exclusion accounts list
1004	Excluded account removed from exclusion accounts list
1005	Excluded account event class added to monitoring
1006	Excluded account event class removed from monitoring
1007	Excluded account facility added to monitoring
1008	Excluded account facility removed from monitoring
1101	Service auditing template added
1102	Service auditing template removed
1103	Service added to auditing template
1104	Service removed from auditing template
1105	Auditing enabled for service
1106	Auditing disabled for service
1107	Service auditing template enabled
1108	Service auditing template disabled
1109	Service auditing template changed
1110	Auditing enabled for SQL instance
1111	Auditing disabled for SQL instance
1112	SQL auditing template enabled
1113	SQL auditing template disabled
1115	SQL auditing template added
1116	SQL auditing template removed
1118	SQL instance added
1119	SQL instance removed
1120	SQL event added
1121	SQL event removed
1122	SQL filter added
1123	SQL filter removed
1124	Active Directory Federation Services auditing template added
1125	Active Directory Federation Services auditing template removed
1126	Active Directory Federation Services auditing template enabled
1127	Active Directory Federation Services auditing template disabled
1128	Active Directory Federation Services sign-in auditing enabled
1129	Active Directory Federation Services sign-in auditing disabled
1130	Active Directory Federation Services auditing template added to agent configuration
1131	Active Directory Federation Services auditing template removed from agent configuration
1132	Active Directory Federation Services configuration changes auditing enabled
1133	Active Directory Federation Services configuration changes auditing disabled
1302	Agent service has reached a critical load
1303	Agent service has more than 100 events waiting
1304	Agent service has returned to normal operations

Table 8. Change Auditor Coordinator Service event log events

Event ID	Description
1401	Exchange mailbox added to monitoring
1402	Exchange mailbox removed from monitoring
1403	Exchange mailbox attribute changed
1404	Exchange protection template added
1405	Exchange protection template removed
1406	Exchange protection template enabled
1407	Exchange protection template disabled
1408	Exchange container added to protection template
1409	Exchange container removed from protection template
1410	Protection for Exchange container enabled
1411	Protection for Exchange container disabled
1412	Override account added to Exchange protection template
1413	Override account removed from Exchange protection template
1414	AD query container added
1415	AD query container removed
1416	AD query container enabled
1417	AD query container disabled
1419	Exchange mailbox enabled
1420	Exchange mailbox disabled
1430	Change Auditor Agent started
1431	Change Auditor Agent stopped
1432	Change Auditor Agent restarted
1433	Change Auditor Agent set uninstalled
1434	Change Auditor Coordinator set uninstalled
1435	Override accounts Exchange protection template Allow
1436	Override accounts Exchange protection template Deny
1440	Exchange user defined shared mailbox added
1441	Exchange user defined shared mailbox removed
1442	Exchange user defined shared mailbox attribute changed
1443	Exchange user defined shared mailbox enabled
1444	Exchange user defined shared mailbox disabled
1445	Exchange shared mailbox auto detection enabled
1446	Exchange shared mailbox auto detection disabled
1600	User added
1601	User deleted
1602	User restored
1603	License properties set
1604	User password reset
1605	User password changed
1606	User license changed
1607	User updated
1608	Force change user password property set

Table 8. Change Auditor Coordinator Service event log events

Event ID	Description
1609	User AccountEnabled property changed
1610	User AssignedLicense property changed
1611	User AssignedPlan property changed
1612	User Mobile property changed
1613	User OtherMail property changed
1614	User StrongAuthenticationMethod property changed
1615	User StrongAuthenticationUserDetails property changed
1616	User TelephoneNumber property changed
1617	User LicenseAssignmentDetail property changed
1618	User OtherMobile property changed
1619	User StrongAuthenticationRequirement property changed
1620	User StrongAuthenticationPhoneApp detail property changed
1621	User AlternativeSecurityId property changed
1622	User PreferredDataLocation property changed
1623	User ProxyAddresses property changed
1624	User UserPrincipalName property changed
1625	User UserState property changed
1626	User UserStateChangedOn property changed
1627	User UserType property changed
1628	User StsRefreshTokensValidFrom property changed
1629	User MSExchRemoteRecipientType property changed
1630	Update user credentials
1631	Microsoft Entra- User event
1632	Group added
1633	Group updated
1634	Group deleted
1635	Group member added
1636	Member added to group
1637	Group member removed
1638	Member removed from group
1639	Group owner added
1640	Owner added to group
1641	Group owner removed
1642	Owner removed from group
1643	Set group to be managed by user
1644	Set group license
1645	Microsoft Entra - Group event
1646	Group Description property changed
1647	Group DisplayName property changed
1648	Group GroupType property changed
1649	Group IsPublic property changed
1650	Group MailNickName property changed

Table 8. Change Auditor Coordinator Service event log events

Event ID	Description
1651	Group SecurityEnabled property changed
1652	Group MembershipRule property changed
1653	Group MembershipRuleProcessingState property changed
1654	Service principal added
1655	Service principal removed
1656	Service principal credentials added
1657	Service principal credentials removed
1658	Delegation entry added
1659	Delegation entry updated
1660	Delegation entry removed
1661	Add owner to application
1662	Microsoft Entra - Application event
1663	Role member added
1664	Role assigned to member
1665	Role member removed
1666	Role removed from member
1667	Eligible member added to role
1668	Role assigned to eligible member
1669	Eligible member removed from role
1670	Role removed from eligible member
1671	Role enabled
1672	Batch invites uploaded
1673	Batch invites proceeded
1674	External user invited
1675	External user invite redeemed
1676	External user added to group
1677	External user assigned to application
1678	Viral tenant created
1679	Viral user created
1680	Microsoft Entra - B2B event
1681	Partner added to company
1682	Partner removed from company
1683	Domain added to company
1684	Domain removed from company
1685	Domain updated
1686	Domain authentication set
1687	Domain federation settings set
1688	Domain verified
1689	Domain verified by email
1690	DirSyncEnabled flag set on company
1691	Password policy set
1692	Company information set

Table 8. Change Auditor Coordinator Service event log events

Event ID	Description
1693	Company contact information set
1694	Microsoft Entra - Directory event
1695	Microsoft Entra - Policy event
1696	Microsoft Entra - Resource event
1697	Microsoft Entra - Administrative Units event
1698	Microsoft Entra - Role event
1699	Microsoft Entra audit event
1700	Successful Microsoft Entra sign-in
1701	Failed Microsoft Entra sign-in
1702	Microsoft Entra sign-in event
1703	Active risk event detected
1704	Closed risk event detected
1705	Active risk event status changed to closed
1706	Closed risk event status changed to active
2001	NetApp auditing template added
2002	NetApp auditing template removed
2003	NetApp path changed in auditing template
2004	NetApp path added to auditing template
2005	NetApp path removed from auditing template
2006	Agent added to NetApp auditing template
2007	Agent removed from NetApp auditing template
2009	NetApp auditing template enabled
2010	NetApp auditing template disabled
2011	Auditing enabled for NetApp path
2012	Auditing disabled for NetApp path
2101	EMC auditing template added
2102	EMC auditing template removed
2103	EMC path changed in auditing template
2104	EMC path added to auditing template
2105	EMC path removed from auditing template
2106	Agent added to EMC auditing template
2107	Agent removed from EMC auditing template
2108	EMC auditing cepp.conf changed
2109	EMC auditing template enabled
2110	EMC auditing template disabled
2111	Auditing enabled for EMC path
2112	Auditing disabled for EMC path
2301	SharePoint auditing template added
2302	SharePoint auditing template removed
2303	Agent added to SharePoint auditing template
2304	Agent removed from SharePoint auditing template
2305	SharePoint auditing template enabled

Table 8. Change Auditor Coordinator Service event log events

Event ID	Description
2306	SharePoint auditing template disabled
2307	Auditing enabled for SharePoint path
2308	Auditing disabled for SharePoint path
2309	SharePoint path changed in auditing template
2310	SharePoint path added to auditing template
2311	SharePoint path removed from auditing template
2312	SharePoint event added
2313	SharePoint event removed
2314	SharePoint facility added
2315	SharePoint facility removed
2316	SQL facility added
2317	SQL facility removed
2601	Microsoft 365 Exchange Online auditing template added
2602	Microsoft 365 Exchange Online auditing template removed
2609	Microsoft 365 Exchange Online auditing template enabled
2610	Microsoft 365 Exchange Online auditing template disabled
2611	Microsoft 365 Exchange Online auditing template was modified
3101	Microsoft Entra auditing template was added
3102	Microsoft Entra auditing template was modified
3103	Microsoft Entra auditing template was removed
3104	Microsoft Entra auditing template was enabled
3105	Microsoft Entra auditing template was disabled
9901	SDK Facility added
9902	SDK Facility removed
9903	SDK Facility modified
9904	SDK Event Class added
9905	SDK Event Class removed
9906	SDK Event Class modified
9907	SDK Agent added
9908	SDK Machine added

Change Auditor Service event log

The Change Auditor Service event log contains the following types of events depending on the event logging enabled in Change Auditor:

- Registry events
- Local Groups events
- Service events

Registry events

The following table lists the events that will be recorded to the Change Auditor Service event log when **Registry** event logging is enabled in Change Auditor.

Table 9. Change Auditor Service event log: Registry events

Event ID	Description
101	Binary registry value added
102	Binary registry value changed
103	Binary registry value deleted
104	Numeric registry value added
105	Numeric registry value changed
106	Numeric registry value deleted
107	String registry value added
108	String registry value changed
109	String registry value deleted
110	Registry key added
111	Registry key deleted

Local Groups events

The following table lists the events that will be recorded to the Change Auditor Service event log when **Local Account** event logging is enabled in Change Auditor.

Table 10. Change Auditor Service event log: Local Groups events

Event ID	Description
201	Local group added
202	Local group removed
203	Local group renamed
204	Member added to local group
205	Member removed from local group
301	Account disabled for local user
302	Account enabled for local user
303	Account expiration change for local user
304	Active session limit changed for local user
305	Allow reconnection option changed for local user
306	Can’t change password option changed for local user
307	Connect client drives at logon option changed for local user
308	Connect client printers at logon option changed for local user
309	Default to main client printer option changed for local user
310	Deny this user terminal services permission changed for local user
311	Dial-in callback number changed for local user
312	Dial-in callback options changed for local user
313	Dial-in static IP address changed for local user
314	Dial-in static routes changed for local user
315	Dial-in verify caller-ID changed for local user

Table 10. Change Auditor Service event log: Local Groups events

Event ID	Description
316	Disconnected session timeout changed for local user
317	Enable remote control changed for local user
318	Home folder mapped drive changed for local user
319	Home folder path changed for local user
320	Idle session limit changed for local users
321	Local user account locked
322	Local user account unlocked
323	Local user added
324	Local user badPwdCount changed
325	Local user logged on
326	Local user removed
327	Local user renamed
328	Logon program filename changed for local user
329	Logon program folder changed for local user
330	Logon script changed for local user
331	Must change password at next logon option changed for local user
332	Password changed for local user
333	Password never expires option changed for local user
334	Password required option changed for local user
335	Profile path changed for local user
336	Remote access permission changed for local user
337	Remote control level of control option changed for local user
338	Remote control require user's permission option changed for local user
339	Session limit action changed for user
340	Start the following program at logon option changed for local user
341	Terminal services home folder mapped drive change for local user
342	Terminal services home folder path changed for local user
343	Terminal services profile path changed for local user

Service events

The following table lists the events the will be recorded to the Change Auditor Service event log when **Service** event logging is enabled in Change Auditor.

Table 11. Change Auditor Service event log: Service events

Event ID	Description
401	Service account changed
402	Service dependencies changed
403	Service paused
404	Service recovery actions changed
405	Service resumed
406	Service start type changed

Table 11. Change Auditor Service event log: Service events

Event ID	Description
407	Service started
408	Service stopped

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.