Quest

Quest® Change Auditor for Microsoft 365® and Microsoft Entra ID ® 7.6.1

Event Reference Guide

© 2025 Quest Software Inc.

ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Quest Software Inc.

The information in this document is provided in connection with Quest Software products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Quest Software products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, QUEST SOFTWARE ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL QUEST SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF QUEST SOFTWARE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Quest Software makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Quest Software does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc.
Attn: LEGAL Dept.
20 Enterprise, Suite 100
Aliso Viejo, CA 92656

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

Patents

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

Trademarks

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

Legend

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

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

Micosoft 365 and Microsoft Entra ID Auditing Event Reference Guide
Updated - September 2025
Software Version - 7.6.1

Contents

Introduction **4**

Events **5**
Microsoft 365 Exchange Online Administration 5
Microsoft 365 Exchange Online Mailbox 6
Microsoft 365 SharePoint Online 9
Microsoft 365 OneDrive for Business 10
Microsoft Entra 12
Microsoft Entra Sign-Ins 17
Microsoft Entra Sign-in Risk Event 17

About us **18**
Our brand, our vision. Together. 18
Contacting Quest 18
Technical support resources 18

1

Introduction

Change Auditor provides in-depth forensics and comprehensive auditing on all key configuration, user and administrator changes in your environments. Information for on-premises and cloud directories can be correlated to provide single pane-of-glass view of your synchronized Active Directory environment and Microsoft 365 organization and making it easy to search events regardless of where they occurred.

To ensure compliance, you can automatically generate intelligent and in-depth reports, protecting you against policy violations and avoiding the risks and errors associated with day-to-day modifications.

Change Auditor audits Exchange Online, SharePoint Online, and OneDrive for Business activities that correspond to the events in the Microsoft 365 Security & Compliance Center audit log and Microsoft Entra ID activities that correspond to the events in the Microsoft Entra ID Audit logs, Sign-in activity report, and Risky sign-ins report.

This guide lists the Microsoft 365 and Microsoft Entra events that can be captured when you have licensed Change Auditor for Exchange, Change Auditor for SharePoint, Change Auditor for Active Directory, and Change Auditor for Logon Activity User. Separate event reference guides are provided that list the core Change Auditor events (when any Change Auditor license is applied) and the events captured when the different auditing modules are licensed.

1

Events

This section lists the audited events specific to Microsoft 365 Exchange Online, SharePoint Online, OneDrive for Business, and Microsoft Entra ID and each event's corresponding severity setting.

- Microsoft 365 Exchange Online Administration
- Microsoft 365 Exchange Online Mailbox
- Microsoft 365 SharePoint Online
- Microsoft 365 OneDrive for Business
- Microsoft Entra
- Microsoft Entra Sign-Ins
- Microsoft Entra Sign-in Risk Event

IMPORTANT: When expecting large numbers of events, you may need to increase the Max Events per Connection setting (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 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 required license.

Microsoft 365 Exchange Online Administration

Table 1. Microsoft 365 Exchange Online Administration events

Event	Description	Severity
Microsoft 365 Exchange Online administrative cmdlet executed	Created when an administrator runs a remote PowerShell command on an object in the Exchange Online mailbox. This can occur as a result of a remote PowerShell connection to the mailbox, or indirectly as a result of an action in the web administration portal for the Microsoft 365 Exchange Online organization.	Medium
Microsoft 365 Exchange Online administrative cmdlet executed by external user	Created when an external user (for example, a Microsoft datacenter personnel or a datacenter service account) runs a remote PowerShell command on an object in the Exchange Online mailbox.	Low

Microsoft 365 Exchange Online Mailbox

NOTE: Inbox rule events are only seen in Change Auditor when they are generated in Outlook.

NOTE: Calendar delegation events are only seen in Change Auditor when they are generated through an OWA client.

Table 2. Microsoft 365 Exchange Online Mailbox events

Event	Description	Severity
Calendar delegation added to online mailbox by owner	Created when calendar delegation is added to an online mailbox by the owner. (Disabled by default.)	Low
Calendar delegation removed from online mailbox by owner	Created when calendar delegation is removed from an online mailbox by the owner. (Disabled by default.)	Low
Folder moved in online mailbox by non-owner	Created when a folder was moved in an online mailbox by a user other than the owner.	Medium
Folder moved in online mailbox by owner	Created when a folder was moved in an online mailbox by the owner. (Disabled by default.)	Low
Folder moved in online shared mailbox	Created when a folder was moved in an online shared mailbox.	Medium
Folder moved to Deleted Items in online mailbox by owner	Created when a folder was moved to the Deleted Items folder in an online mailbox by the owner. (Disabled by default.)	Low
Folder moved to Deleted Items in online shared mailbox	Created when a folder was moved to the Deleted Items folder in an online shared mailbox.	Medium
Folder moved to Deleted Items in online mailbox by non-owner	Created when a folder was moved to the Deleted Items folder in an online mailbox by a user other than the owner.	Medium
Folder opened in online mailbox by non-owner	Created when a folder is opened in a user's mailbox by a user other than the owner.	Medium
Folder opened in online mailbox by owner	Created when a folder is opened in a user's mailbox by its owner.	Low
Folder opened in online shared mailbox	Created when a folder is opened in an online shared mailbox.	Medium
Folder opened in online mailbox by owner	Created when a folder is opened in an online mailbox by owner. (Disabled by default.)	Low
Folder permissions added in online mailbox by owner	Created when folder permissions are added to an online mailbox by owner. (Disabled by default.)	Low
Folder permissions added in online mailbox by non-owner	Created when folder permissions are added to an online mailbox by a user other than the owner.	Medium
Folder permissions added in online shared mailbox	Created when folder permissions are added to an online shared mailbox by a user other than the owner.	Medium
Folder permissions modified in online mailbox by owner	Created when folder permissions are modified in an online mailbox by owner. (Disabled by default.)	Low
Folder permissions modified in online mailbox by non-owner	Created when folder permissions are modified in an online mailbox by a user other than the owner.	Medium
Folder permissions modified in online shared mailbox	Created when folder permissions are modified in an online shared mailbox by a user other than the owner.	Medium
Folder permissions removed in online mailbox by owner	Created when folder permissions are removed from an online mailbox by owner. (Disabled by default.)	Low
Folder permissions removed in online mailbox by non-owner	Created when folder permissions are removed from an online mailbox by a user other than the owner.	Medium
Folder permissions removed in online shared mailbox	Created when folder permissions are removed in an online shared mailbox by a user other than the owner.	Medium

Table 2. Microsoft 365 Exchange Online Mailbox events

Event	Description	Severity
Folder synchronized from online mailbox by owner.	Created when emails are synchronized in an online mailbox by the owner. (Disabled by default.) **NOTE:** A Microsoft 365 E5 license is required to audit this activity.	Low
Folder synchronized from online mailbox by non-owner.	Created when emails are synchronized in an online mailbox by a user other than the owner. **NOTE:** A Microsoft 365 E5 license is required to audit this activity.	Medium
Folder synchronized from online shared mailbox	Created when a emails are synchronized from a shared mailbox. (Disabled by default.) **NOTE:** A Microsoft 365 E5 license is required to audit this activity.	Medium
Inbox rule added to online mailbox by owner	Created when inbox rules are added in an online mailbox by owner. (Disabled by default.)	Low
Inbox rule added to online mailbox by non-owner	Created when inbox rules are added in an online mailbox by a user other than the owner.	Medium
Inbox rule added in online shared mailbox	Created when inbox rules are added in an online shared mailbox.	Medium
Inbox rule modified in online mailbox by owner	Created when inbox rules are updated in an online mailbox by owner. (Disabled by default.)	Low
Inbox rule modified in online mailbox by non-owner	Created when inbox rules are updated in an online mailbox by a user other than the owner.	Medium
Inbox rule modified in online shared mailbox	Created when inbox rules are updated in an online shared mailbox.	Medium
Inbox rule removed from online mailbox by owner	Created when inbox rules are removed from an online mailbox by owner. (Disabled by default.)	Low
Inbox rule removed from online mailbox by non owner	Created when inbox rules are removed from an online mailbox by a user other than the owner.	Medium
Inbox rule removed from online shared mailbox	Created when inbox rules are removed from an online shared mailbox.	Medium
Online mailbox auditing has been throttled	Created when Microsoft throttles the mailbox after 1000 mail items have been accessed. Message opened events will not be recorded for 24 hours. **NOTE:** A Microsoft 365 E5 license is required to audit this activity.	Medium
Message copied in online mailbox by non-owner	Created when a message is copied from one folder to another in a user's online mailbox by a user other than the owner.	Medium
Message copied in online shared mailbox	Created when a message is copied from one folder to another in an online shared mailbox.	Medium
Message created in online mailbox folder by non-owner	Created when a new message is created in a user's mailbox by a user other than the owner.	Medium
Message created in online shared mailbox	Created when a new message is created in an online shared mailbox by a user other than the owner.	Medium
Message created in online mailbox by owner	Created when a message was created in a folder in an online mailbox by the mailbox owner. (Disabled by default.)	Low
Message hard-deleted in an online mailbox by non-owner	Created when a message is purged from a user's Deleted Items list by a user other than the owner.	Medium
Message hard-deleted in online mailbox by owner	Created when a message was hard-deleted from an online mailbox by the mailbox owner. (Disabled by default.)	Low

Table 2. Microsoft 365 Exchange Online Mailbox events

Event	Description	Severity
Message hard-deleted in online shared mailbox	Created when a message is purged from an online shared mailbox.	Medium
Message moved in online mailbox by non-owner	Created when a message is moved from one folder to another in a user's mailbox by a user other than the owner.	Medium
Message moved in online mailbox by owner	Created when a message was moved in an online mailbox by the mailbox owner. (Disabled by default.)	Low
Message moved in online shared mailbox	Created when a message is moved from one folder to another in an online shared mailbox.	Medium
Message moved to Deleted Items in online mailbox by non-owner	Created when a message is moved to the Deleted Items folder in a user's online mailbox by a user other than the owner.	Medium
Message moved to Deleted Items in online shared mailbox	Created when a message is moved to the Deleted Items folder in an online shared mailbox.	Medium
Message moved to Deleted Items in online mailbox by owner	Created when a message was moved to the Deleted Items folder in an online mailbox by the mailbox owner. (Disabled by default.)	Low
Message opened in online mailbox by non-owner	Created when a message was opened in a folder in an online mailbox by a user other than the owner. **NOTE:** A Microsoft 365 E5 license is required to audit this activity.	Medium
Message opened in online mailbox by owner	Created when a message was opened in a folder in an online mailbox by its owner. (Disabled by default.) **NOTE:** A Microsoft 365 E5 license is required to audit this activity.	Low
Message opened in online shared mailbox	Created when a message was opened in a folder in an online shared mailbox. (Disabled by default.) **NOTE:** A Microsoft 365 E5 license is required to audit this activity.	Medium
Message sent as another user in online mailbox by owner	Created when a user sends a message as another user from their own online mailbox. (Disabled by default.)	Medium
Message sent as another user in online shared mailbox	Created when a user sends a message as another user from an online shared mailbox.	Medium
Message sent as another user in online mailbox by non-owner	Created when a user other than the owner sends a message as another user from an online mailbox.	Medium
Message sent on behalf of another user in online mailbox by owner	Created when a user sends a message on behalf of another user from their own online mailbox. (Disabled by default.)	Medium
Message sent on behalf of another user in online mailbox by non-owner	Created when a user other than the owner sends a message on behalf of another user from an online mailbox.	Medium
Message sent on behalf of another user in online shared mailbox	Created when a user sends a message as another user from an online shared mailbox.	Medium
Message soft-deleted in online mailbox by non-owner	Created when a message is deleted from an online mailbox using the Outlook shift-delete function by non-owner.	Medium
Message soft-deleted in online mailbox by owner	Created when a message is deleted from a user's online mailbox using the Outlook shift-delete function. (Disabled by default.)	Low
Message soft-deleted in online shared mailbox	Created when a message is deleted from an online shared mailbox using the Outlook shift-delete function.	Medium

Table 2. Microsoft 365 Exchange Online Mailbox events

Event	Description	Severity
Message updated in online mailbox by non-owner	Created when certain message properties were changed in a user's mailbox by a user other than the owner.	Medium
Message updated in online mailbox by owner	Created when message updated in online mailbox by owner. (Disabled by default.)	Low
Message updated in online shared mailbox	Created when certain message properties were changed in online shared mailbox.	Medium
Online Mailbox login by owner	Created when a mailbox owner logs in to an online mailbox.	Low
Microsoft 365 Exchange Online Mailbox event	Generic Exchange Online Mailbox event with a dynamically constructed event description (What statement). The event is created when Exchange Online Mailbox activity is detected that does not have a corresponding event defined in Change Auditor.	Low

Microsoft 365 SharePoint Online

Table 3. SharePoint Online group events

Event	Description	Severity
Group member added in SharePoint Online	Created when a member is added to a SharePoint Online group. The target for this event is the group.	Medium
Group member removed in SharePoint Online	Created when a member is removed from a SharePoint Online group. The target for this event is the group.	Medium
Member added to group in SharePoint Online	Created when a member is added to a SharePoint Online group. The target for this event is the member.	Medium
Member removed from group in SharePoint Online	Created when a member is removed from a SharePoint Online group. The target for this event is the member.	Medium

Table 4. Microsoft 365 SharePoint Online file events

Event	Description	Severity
File accessed in SharePoint Online	Created when a user or system account accesses a file in a SharePoint Online site.	Low
File checked in in SharePoint Online	Created when a user checks a file back in to a document library after they have completed their edits.	Medium
File checked out and discarded in SharePoint Online	Created when a file check out is undone resulting in no edits to the file in the document library.	Medium
File checked out in SharePoint Online	Created when a user checks out a file from a document library to ensure it is not accessed by others while being edited.	Medium
File copied in SharePoint Online	Created when a file is copied in a SharePoint Online site.	Medium
File deleted in SharePoint Online	Created when a file is deleted from a SharePoint Online site.	Medium
File downloaded in SharePoint Online	Created when a file is downloaded from a SharePoint Online site.	Medium
File modified in SharePoint Online	Created when file contents or properties are changed by a user or system account in a SharePoint Online site.	Medium
File moved in SharePoint Online	Created when a file is moved in a SharePoint Online site.	Medium

Table 4. Microsoft 365 SharePoint Online file events

Event	Description	Severity
File previewed in SharePoint Online	Created when a file is viewed by a user or system account in a SharePoint Online site.	Low
File renamed in SharePoint Online	Created when a file is renamed in a SharePoint Online site.	Medium
File restored in SharePoint Online	Created when a deleted file is restored in a SharePoint Online site.	Medium
File uploaded in SharePoint Online	Created when a file is uploaded to a SharePoint Online site.	Medium

Table 5. Microsoft 365 SharePoint Online folder events

Event	Description	Severity
Folder accessed in SharePoint Online	Created when a user or system account accesses a folder in a SharePoint Online site.	Low
Folder created in SharePoint Online	Created when a folder is created in a SharePoint Online site.	Medium
Folder deleted in SharePoint Online	Created when a folder is deleted from a SharePoint Online site.	Medium
Folder modified in SharePoint Online	Created when a folder's properties are changed in a SharePoint Online site.	Medium
Folder moved in SharePoint Online	Created when a folder is moved in a SharePoint Online site.	Medium
Folder renamed in SharePoint Online	Created when a folder is renamed in a SharePoint Online site.	Medium

Table 6. SharePoint Online event

Event	Description	Severity
Microsoft 365 SharePoint Online event	Generic SharePoint Online event with a dynamically constructed event description (What statement). The event is created when SharePoint Online activity is detected that does not have a corresponding event defined in Change Auditor.	Low

Microsoft 365 OneDrive for Business

Table 7. Microsoft 365 OneDrive for Business file events

Event	Description	Severity
File accessed in OneDrive for Business	Created when a user or system account accesses a file in a OneDrive for Business site.	Low
File checked in in OneDrive for Business	Created when a user checks in a file to a document library.	Medium
File checked out and discarded in OneDrive for Business	Created when a file check out is undone resulting in no edits to the file in the document library.	Medium
File checked out in OneDrive for Business	Created when a user checks out a file from a document library.	Medium
File copied in OneDrive for Business	Created when a file is copied in a OneDrive for Business site.	Medium
File deleted in OneDrive for Business	Created when a file is deleted from a OneDrive for Business site.	Medium

Table 7. Microsoft 365 OneDrive for Business file events

Event	Description	Severity
File downloaded in OneDrive for Business	Created when a file is downloaded from a OneDrive for Business site.	Medium
File modified in OneDrive for Business	Created when file contents or properties are changed by a user or system account in a OneDrive for Business site.	Medium
File moved in OneDrive for Business	Created when a file is moved in a OneDrive for Business site.	Medium
File previewed in OneDrive for Business	Created when a user or system account views a file in a OneDrive for Business site.	Low
File renamed in OneDrive for Business	Created when a file is renamed in a OneDrive for Business site.	Medium
File restored in OneDrive for Business	Created when a deleted file is restored in a OneDrive for Business site.	Medium
File synchronized from a local OneDrive folder to OneDrive for Business	Created when a file is uploaded to a remote OneDrive folder from local OneDrive folder.	Low
File synchronized from OneDrive for Business to a local OneDrive folder	Created when a file is uploaded to a remote OneDrive folder from a local OneDrive folder.	Low
File uploaded in OneDrive for Business	Created when a file is uploaded to a OneDrive for Business site.	Medium

Table 8. Microsoft 365 OneDrive for Business folder events

Event	Description	Severity
Folder accessed in OneDrive for Business	Created when a user or system account accesses a folder in a OneDrive for Business site.	Low
Folder created in OneDrive for Business	Created when a folder is created in a OneDrive for Business site.	Medium
Folder deleted in OneDrive for Business	Created when a folder is deleted from a OneDrive for Business site.	Medium
Folder modified in OneDrive for Businesse	Created when a folder's properties are changed in a OneDrive for Business site.	Medium
Folder moved in OneDrive for Business	Created when a folder is moved in a OneDrive for Business site.	Medium
Folder renamed in OneDrive for Business	Created when a folder is renamed in a OneDrive for Business site.	Medium

Table 9. Microsoft 365 OneDrive for Business event

Event	Description	Severity
Microsoft 365 OneDrive for Business event	Generic OneDrive for Business event with a dynamically constructed event description (What statement). The event is created when OneDrive for Business activity is detected that does not have a corresponding event defined in Change Auditor.	Low

Microsoft Entra

Change Auditor audits activities in Microsoft Entra ID that correspond to the events in the Audit logs in the Microsoft Entra admin center.

Table 10. Microsoft Entra User events

Event	Description	Severity
User added	Created when a user is added to the directory.	Medium
User deleted	Created when a user is deleted from the directory.	Medium
User restored	Created when a user is restored in the directory.	Medium
User updated	Created when a user account is updated. See User attribute events.	Medium
License properties set	Created when the Global Administrator assigns a license for a particular plan to a user in the directory.	Medium
User license changed	Created when the license assigned to a user in the directory is changed. See User license attributes events.	Medium
User password changed	Created when the password for a user in the directory is changed.	Medium
User password reset	Created when the password for a user in the directory is reset.	Medium
Microsoft Entra - User event	Generic user event with a dynamically constructed event description (What statement). The event is created when user activity is detected that does not have a corresponding event defined in Change Auditor.	Medium

Table 11. User attribute events

Event	Description	Severity
User AccountEnabled property changed	Created when a user's sign-in status is changed. (Administrators can set the status to allowed and blocked.)	Medium
User AlternativeSecurityId property changed	Created when a user's alternate security ID is changed as part of the Microsoft Entra external account workflow.	Medium
User PreferredDataLocation property changed	Created when the preferred location for the user data is changed.	Medium
User Mobile property changed	Created when a user's mobile phone number is changed.	Medium
User MSExchRemoteRecipientType property changed	Created when mailbox type is changed. For example, an on-premises mailbox was migrated to Exchange Online or archive mailbox was added.	Medium
User OtherMail property changed	Created when a user's alternate email address is changed.	Medium
User OtherMobile property changed	Created when a user's alternate mobile phone number is changed.	Medium
User ProxyAddresses property changed	Created when one of the user proxy addresses is changed, added, or removed.	Medium
User TelephoneNumber property changed	Created when a user's telephone number is changed.	Medium
User StrongAuthenticationMethod property changed	Created when the multi-factor authentication for verification method has been changed for a user. Available methods include call to phone, text message to phone, notification through mobile application, and verification code from mobile application.	Medium
User StrongAuthenticationPhoneAppDetail property changed.	Created when a user's phone application used for multi-factor authentication and password reset verification have been changed	Medium
User StrongAuthenticationUserDetail property changed	Created when a user's phone number, alternative phone number, or email address used for multi-factor authentication and password reset verification have been changed.	Medium
User StrongAuthenticationRequirement property changed	Created when multi-factor authentication is enforced, enabled, or disabled for a user. Turning on multi-factor authentication changes the state to enabled. The state changes to enforced when the user signs in and authenticates.	Medium
User StsRefreshTokensValidFrom property changed	Created when a user's StsRefreshTokenValidFrom property is changed. For example, when a user's authorization token should be invalidated.	Medium
User UserPrincipalName property changed	Created when the UPN for a user account is changed.	Medium
User UserType property changed	Created when the user type is changed. The available type includes member, guest, or viral.	Medium
User UserStateChangedOn property changed	Created when the timestamp of the last change to the UserState is changed as part of the Microsoft Entra external account workflow.	Medium
User UserState property changed	Created when the user state is changed as part of the Microsoft Entra external account workflow. (PendingApproval/PendingAcceptance/Accepted/ PendingVerification)	Medium

Table 12. User license attributes events

Event	Description	Severity
Force change user password property set	Created when the property that requires a user to change their password is set.	Medium
User AssignedLicense property changed	Created when a user's product licenses has been edited. (Administrators can assign, reassign, or remove licenses as required.)	Medium
User AssignedPlan property changed	Created when a licensed user's assigned plan details are changed.	Medium
User LicenseAssignmentDetail property changed	Created when the license detail assigned to a user is changed.	Medium

Table 13. Microsoft Entra Role events

Event	Description	Severity
Eligible member added to role	Created when an eligible member is added to a role.	High
Eligible member removed from role	Created when an eligible member is removed from a role.	High
Role assigned to eligible member	Created when an eligible member is added to a role.	High
Role assigned to member	Created when a member is added to a role.	High
Role member added	Created when a user or service principal is added to a directory role.	High
Role member removed	Created when a user or service principle is removed from a directory role.	High
Role removed from eligible member	Created when an eligible member is removed from a role.	High
Role removed from member	Created when a member is removed from a role.	High
Microsoft Entra - Role event	Generic user event with a dynamically constructed event description (What statement). The event is created when user activity is detected that does not have a corresponding event defined in Change Auditor.	Medium

Table 14. Microsoft Entra Active Group events

Group Property changes are monitored for the following types of groups: Microsoft 365, Distribution list, and Security groups.

Event	Description	Severity
Group added	Created when a group is created in the directory.	Medium
Group deleted	Created when a group is deleted from the directory.	Medium
Group member added	Created when a member is added to a group in the directory.	Medium
Group member removed	Created when a member is removed from a group in the directory.	Medium
Group owner added	Created when an owner is added to a group in the directory.	Medium
Group owner removed	Created when an owner is removed from a group in the directory.	Medium
Group updated	Created when a group is updated. See Group attributes events.	Medium
Member added to group	Created when a member is added to a group.	Medium
Member removed from group	Created when a member is removed from a group.	Medium
Owner added to group	Created when an owner is added to a group.	Medium
Owner removed from group	Created when an owner is removed from a group.	Medium

Event	Description	Severity
Set group to be managed by user	Created when a group is set to be managed by a user in the directory.	Medium
Set group license	Created when a license is assigned to a group in the directory.	Medium
Microsoft Entra - Group event	Generic group event with a dynamically constructed event description (What statement). The event is created when group activity is detected that does not have a corresponding event defined in Change Auditor.	Medium

Table 15. Group attributes events

Event	Description	Severity
Group Description property changed	Created when the group description is changed.	Low
Group DisplayName property changed	Created when the group display name (friendly name) is changed.	Medium
Group GroupType property changed	Created when the group type (Microsoft 365, Distribution List, or Security) and the group membership type (assigned or dynamic) is changed. **NOTE:** • Microsoft 365 groups have a group type property of 'Unified' and security groups and distribution lists display an empty group type. • If the Group Membership assignment is dynamic, the group type property displays DynamicMembership'. If the Group Membership is assigned, the group type property is empty.	Medium
Group IsPublic property changed	Created when the group privacy setting (public or private) is changed.	High
Group MailNickName property changed	Created when the group alias is changed.	Medium
Group MembershipRule property changed	Created when the criteria that determines which members should belong to a dynamic group is changed. **NOTE:** This option is only available with an Microsoft Entra ID premium license and is set through configuring a group's dynamic membership settings.	High
Group MembershipRuleProcessingState property changed	Created when the status of membership processing state is changed for a group. **NOTE:** This value can only be changed through PowerShell.	High
Group SecurityEnabled property changed	Created when the property that determined whether a group is security enabled is changed.	Medium
Set group to be managed by user	Created when a group is set to be managed by a user in the directory.	Medium

Table 16. Microsoft Entra Application event

Event	Description	Severity
Microsoft Entra - Application event	Generic application event with a dynamically constructed event description (What statement). The event is created when application activity is detected that does not have a corresponding event defined in Change Auditor.	Medium

Table 17. Microsoft Entra Resource event

Event	Description	Severity
Microsoft Entra - resource event	Generic resource event with a dynamically constructed event description (What statement). The event is created when resource activity is detected that does not have a corresponding event defined in Change Auditor.	Low

Table 18. Microsoft Entra Directory event

Event	Description	Severity
Microsoft Entra - Directory event	Generic directory event with a dynamically constructed event description (What statement). The event is created when directory activity is detected that does not have a corresponding event defined in Change Auditor.	Medium

Table 19. Microsoft Entra Policy event

Event	Description	Severity
Microsoft Entra - Policy Directory event	Generic policy event with a dynamically constructed event description (What statement). The event is created when policy activity is detected that does not have a corresponding event defined in Change Auditor.	Low

Table 20. Microsoft Entra event

Event	Description	Severity
Microsoft Entra audit event	Created when Microsoft Entra activity is generated that does not have a corresponding event defined in Change Auditor.	Low

Microsoft Entra Sign-Ins

Change Auditor audits activities in the Microsoft Entra that correspond to the events in the Sign-ins report in the Microsoft Entra admin centerl.

Table 21. Microsoft Entra Sign-in events

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

Microsoft Entra Sign-in Risk Event

Change Auditor audits activities in the Microsoft Entra that correspond to the events in the Risky sign-ins report in the Microsoft Entra admin center.

Table 22. Microsoft Entra Sign-in risk events

Event	Description	Severity
Active risk event detected	Created when a new risk event is detected with an active state.	High
Active risk event status changed to closed	Created when an active risk event is closed as a result of being marked as: • Resolved: The issue has been addressed and has been safely closed. • False positive: The issue has been incorrectly identified as a risk and has been safely closed. • Ignore: The issue has been removed from the active list. This event helps you to understand why a risk event has been manually closed.	Low
Closed risk event status changed to active	Created when a closed risk event is reactivated.	High
Closed risk event detected	Created when a new risk event is detected with a closed state. This can happen if the risk event has been marked as resolved, a false positive, set to ignore, closed (remediated), closed (login blocked), closed (automatic multi-factor authentication), or closed (multiple reasons) before it has been detected by Change Auditor for the first time.	Low

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.