

Office 365® and Azure® Active Directory®
Auditing 7.0

Event Reference Guide



© 2018 Quest Software Inc,

ALL RIGHTS RESERVED.

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

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

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

Quest Software Inc,
Attn: LEGAL Dept.
4 Polaris Way
Aliso Viejo, CA 92656

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


Patents

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

Trademarks

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

Legend

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

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

Contents

| | |
|---|----------|
| Introduction | 4 |
| Events | 5 |
| Office 365 Exchange Online Administration | 5 |
| Office 365 Exchange Online Mailbox | 6 |
| Office 365 SharePoint Online | 8 |
| Office 365 OneDrive for Business | 9 |
| Azure Active Directory | 11 |
| Azure Active Directory Sign-Ins | 16 |
| Azure Active Directory Sign-in Risk Event | 16 |

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 Office 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 Office 365 Security & Compliance Center audit log and Azure Active Directory activities that correspond to the events in the Azure Active Directory Audit logs, Sign-in activity report, and Risky sign-ins report.

This guide lists the Office 365 and Azure Active Directory 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.

Events

This section lists the audited events specific to Office 365 Exchange Online, SharePoint Online, OneDrive for Business, and Azure Active Directory and each event's corresponding severity setting.

- [Office 365 Exchange Online Administration](#)
- [Office 365 Exchange Online Mailbox](#)
- [Office 365 SharePoint Online](#)
- [Office 365 OneDrive for Business](#)
- [Azure Active Directory](#)
- [Azure Active Directory Sign-Ins](#)
- [Azure Active Directory Sign-in Risk Event](#)

i | **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.

i | **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.

Office 365 Exchange Online Administration

Table 1. Office 365 Exchange Online Administration events

| Event | Description | Severity |
|--|---|----------|
| Office 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 Office 365 Exchange Online organization. | Medium |
| Office 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 |

Office 365 Exchange Online Mailbox

Table 2. Office 365 Exchange Online Mailbox events

| Event | Description | Severity |
|--|--|----------|
| 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 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 hard-deleted in online mailbox by non-owner | Created when a folder was hard-deleted from an online mailbox by a user other than the owner. | Medium |
| Folder hard-deleted in online mailbox by owner | Created when a folder was hard-deleted from an online mailbox by the owner. (Disabled by default.) | Low |
| Folder hard-deleted in online shared mailbox | Created when a folder was hard-deleted from a shared online mailbox. | Medium |
| Folder soft-deleted in online mailbox by owner | Created when a folder was soft-deleted from an online mailbox by the owner. (Disabled by default.) | Low |
| Folder soft-deleted in online mailbox by non-owner | Created when a folder was soft-deleted from an online mailbox by a user other than the owner. | Medium |
| Folder soft-deleted in online shared mailbox | Created when a folder is soft-deleted from a shared online mailbox. | 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. Office 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. | Medium |
| Message opened in online shared mailbox | Created when a message was opened in a folder in an online shared mailbox. | Low |
| 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 |
| 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 |

Table 2. Office 365 Exchange Online Mailbox events

| Event | Description | Severity |
|--|---|-----------------|
| Online Mailbox login by owner | Created when a mailbox owner logs in to an online mailbox. | Low |
| Office 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 |

Office 365 SharePoint Online

Table 3. Office 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 |
| 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 4. Office 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 |

Table 4. Office 365 SharePoint Online folder events

| Event | Description | Severity |
|-------------------------------------|---|-----------------|
| 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 5. SharePoint Online event

| Event | Description | Severity |
|------------------------------------|---|-----------------|
| Office 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 |

Office 365 OneDrive for Business

Table 6. Office 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 |
| 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 uploaded in OneDrive for Business | Created when a file is uploaded to a OneDrive for Business site. | Medium |

Table 7. Office 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 Business | 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 8. Office 365 OneDrive for Business event

| Event | Description | Severity |
|--|---|-----------------|
| Office 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 |

Azure Active Directory

Change Auditor audits activities in the Azure Active Directory that correspond to the events in the Audit logs in the Azure Active Directory portal.

Table 9. Azure Active Directory 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 |
| 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 enabled | Created when a directory role is enabled in Azure Active Directory. Directory roles, also known as administrator roles, represent a specific set of rights within Azure Active Directory. Users access to Azure Active Directory features depends on the roles they have been assigned. | Medium |
| Azure Active Directory - 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 10. 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 Azure Active Directory 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 Azure Active Directory external account workflow. | Medium |
| User UserState property changed | Created when the user state is changed as part of the Azure Active Directory external account workflow. (PendingApproval/PendingAcceptance/Accepted/PendingVerification) | Medium |

Table 11. User license attributes events

| Event | Description | Severity |
|---|--|-----------------|
| Force change user password property set | Created when the property that forces 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 12. Azure Active Group events

Group Property changes are monitored for the following types of groups: Office 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 |
| 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 |
| Azure Active Directory - Group event | Generic group event with a dynamically constructed event description (<i>What statement</i>). The event is created when group activity is detected that does not have a corresponding event defined in Change Auditor. | Medium |

Table 13. 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 (Office 365, Distribution List, or Security) and the group membership type (assigned or dynamic) is changed. | Medium |
| <p>NOTE:</p> <ul style="list-style-type: none"> Office 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. | | |
| 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. | High |
| <p>NOTE: This option is only available with an Azure Active Directory premium license and is set through configuring a group's dynamic membership settings.</p> | | |
| Group MembershipRuleProcessingState property changed | Created when the status of membership processing state is changed for a group. | High |
| <p>NOTE: This value can only be changed through PowerShell.</p> | | |
| 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 14. Azure Active Directory Application event

| Event | Description | Severity |
|--|---|----------|
| Azure Active Directory - 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 15. Azure Active Directory Device event

| Event | Description | Severity |
|---------------------------------------|---|----------|
| Azure Active Directory - Device event | Generic device event with a dynamically constructed event description (What statement). The event is created when device activity is detected that does not have a corresponding event defined in Change Auditor. | Low |

Table 16. Azure Active Directory Directory event

| Event | Description | Severity |
|--|---|-----------------|
| Azure Active Directory - 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 17. Azure Active Directory Policy event

| Event | Description | Severity |
|---|---|-----------------|
| Azure Active Directory - 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 18. Azure Active Directory event

| Event | Description | Severity |
|------------------------------------|---|-----------------|
| Azure Active Directory audit event | Created when Azure Active Directory activity is generated that does not have a corresponding event defined in Change Auditor. | Low |

Azure Active Directory Sign-Ins

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

Table 19. Azure Active Directory Sign-in events

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

Azure Active Directory Sign-in Risk Event

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

Table 20. Azure Active Directory Sign-in risk events

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

We are more than just a name

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

Our brand, our vision. Together.

Our logo reflects our story: innovation, community and support. An important part of this story begins with the letter Q. It is a perfect circle, representing our commitment to technological precision and strength. The space in the Q itself symbolizes our need to add the missing piece—you—to the community, to the new Quest.

Contacting Quest

For sales or other inquiries, visit www.quest.com/contact.

Technical support resources

Technical support is available to Quest customers with a valid maintenance contract and customers who have trial versions. You can access the Quest Support Portal at <https://support.quest.com>.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request.
- View Knowledge Base articles.
- Sign up for product notifications.
- Download software and technical documentation.
- View how-to-videos.
- Engage in community discussions.
- Chat with support engineers online.
- View services to assist you with your product.