Quest

Quest® Change Auditor for Microsoft 365® and Microsoft Entra ID ® 7.6.3

User 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.

Microsoft 365 and Microsoft Entra ID Auditing User Guide
Updated - August 2026
Software Version - 7.6.3

Contents

Microsoft 365 and Microsoft Entra ID Auditing Overview 4
Introduction 4
System overview 5
Client components and features 6
Deployment requirements 7
System requirements 8
License requirements 8
Auditing and agent considerations 8
Auditing in synchronized environments 9
Upgrading Change Auditor 9

Configuring Microsoft 365 and Microsoft Entra ID auditing 11
Managing Microsoft 365 templates 12
Microsoft 365 auditing page 12
Create an Microsoft 365 auditing template 13
Edit a Microsoft 365 auditing template 16
Using an existing web application 19
Disable a template 20
Delete a template 20
Managing Microsoft Entra templates 20
Microsoft Entra auditing page 21
Create a Microsoft Entra auditing template 21
Edit a Microsoft Entra auditing template 23
Disable a template 24
Delete a template 25
Considerations 25

Reports and Searches 27
Introduction to Microsoft 365 and Microsoft Entra ID reporting 28
Microsoft 365 built-in reports 28
Microsoft Entra built-in reports 28
Custom searches 28
Creating custom Exchange Online searches 29
Creating a custom SharePoint Online and OneDrive for Business search 31
Creating custom Microsoft Entra searches 32
Additional information for synchronized environments 35
Working with generic Microsoft 365 and Microsoft Entra events 36
Additional Microsoft 365 and Microsoft Entra event details 37

About us 38
Our brand, our vision. Together. 38
Contacting Quest 38
Technical support resources 38

1

Microsoft 365 and Microsoft Entra ID Auditing Overview

- Introduction
- System overview
- Client components and features
- Deployment requirements

Introduction

Change Auditor provides extensive, customizable auditing of critical activities and detailed alerts about vital changes taking place in Microsoft 365 Exchange Online, SharePoint Online, OneDrive for Business, and Microsoft Entra ID. Continually being in-the-know helps you to prove compliance, drive security, and improve uptime while proactively auditing changes to configurations and permissions.

You can generate intelligent, in-depth reports, protecting you against policy violations and avoiding the risks and errors associated with day-to-day modifications. By correlating accounts across the on-premises and cloud environment, you can easily search all events regardless of where they occurred.

Change Auditor's consolidated audit platform, which is not available with system provided tools, enhances your ability to secure your directory and resources. Specifically, Change Auditor provides:

- Detailed information giving you the Who, What, Where, and When for every event.
- Single console and event format across all platforms.
- Standardized search allowing you to search by any key field.
- Consolidated view of on-premises and cloud activity.
- Correlated on-premises and cloud identities for synchronized environments.
- Ability to create alerts on any event for both on-premises and cloud activity.
- Ability to store audit data indefinitely for compliance purposes.

This guide has been prepared to assist you in becoming familiar with auditing Microsoft 365 and Microsoft Entra ID. It is intended for network administrators, consultants, analysts, and any other IT professionals using the product.

- For information on the core functionality available in Change Auditor regardless of the product license that has been applied, see the Change Auditor User Guide and the Change Auditor Installation Guide.
- For event details, see the Microsoft 365 and Microsoft Entra ID Event Reference Guide.

System overview

To audit Microsoft 365 and Microsoft Entra ID, Change Auditor agents require access to the tenant. A web application, which is an Microsoft Entra object, is used to grant this access to external programs, such as Change Auditor.

In addition, to configure and maintain Exchange Online mailbox auditing, Change Auditor agents must be granted access to the Exchange Online organization.

The following describes the integration points and process required for auditing:

1. Users configure an Microsoft 365 or an Microsoft Entra auditing template and select an agent to receive events. The following credentials are required:
   - An account with the Global Administrator role. This account is used to create the web application and assign the required permissions for Change Auditor to perform auditing. After the web application is created, the credentials are no longer used. The agent retrieves the web application ID and key and securely stores them. The agent uses the ID and key to retrieve events from Microsoft 365 and Microsoft Entra ID.
   - For Microsoft 365 Exchange Online auditing, an account with the Exchange Administrator role is also required. This account is used to configure the mailbox auditing settings in the tenant that are defined in the template (such as enabling auditing of owner activity). The agent periodically uses these credentials to validate or update auditing settings, so they are securely stored in Change Auditor.
2. The agent connects to the tenant and creates the web application.

   For Microsoft 365 Exchange Online, the agent also connects to your Exchange Online organization and configures mailbox auditing.
3. The agent periodically gathers events.

   For Microsoft 365 Exchange Online, the agent also retrieves mailbox auditing settings to validate configuration.
4. The agent processes events and forwards them to the coordinator.
5. The coordinator forwards events to the Change Auditor database.

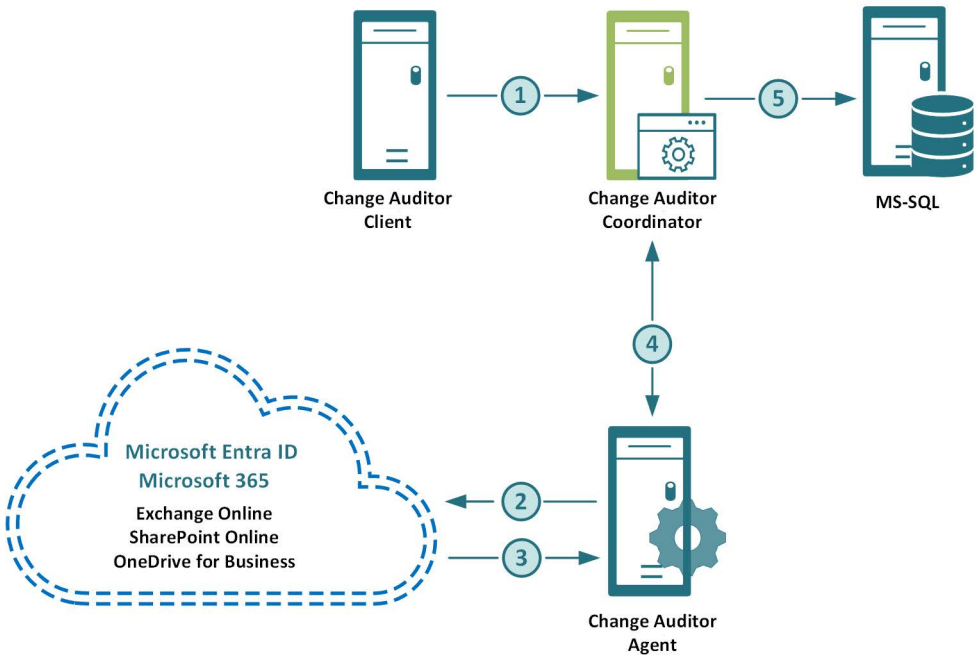

Figure 1. Change Auditor and Microsoft 365/Microsoft Entra ID integration required for auditing

Client components and features

The following table lists the client components and features that require a valid Change Auditor for Exchange, Change Auditor for Active Directory, Change Auditor for SharePoint, and Change Auditor for Logon Activity license. You are not be prevented from using these features; however, associated events are not captured or enforced unless the proper license is applied.

NOTE: To hide unlicensed Change Auditor features from the Administration Tasks tab (including unavailable audit events throughout the client), select **Action | Hide Unlicensed Components**. This command is only available when the Administration Tasks tab is the active page.

Table 1. Client components and features

Client Page	Feature
Administration Tasks Tab	Audit Task List: • Microsoft Entra • Microsoft 365
Event Details Pane	What Details: • Mailbox (Exchange Online Mailbox) • Folder (Exchange Online Mailbox) • Cmdlet (Exchange Online Administration) • Operation (SharePoint Online and OneDrive for Business) • Object (Exchange Online Administration, SharePoint Online, and OneDrive for Business)
Events	Facilities: • Microsoft 365 Exchange Online Administration • Microsoft 365 Exchange Online Mailbox • Microsoft 365 SharePoint Online • Microsoft 365 OneDrive for Business • Microsoft Entra — Application • Microsoft Entra — Administrative Units • Microsoft Entra — Device • Microsoft Entra — Directory • Microsoft Entra — Group • Microsoft Entra — Policy • Microsoft Entra — Risk Event • Microsoft Entra — Role • Microsoft Entra — Sign-in • Microsoft Entra — User • Microsoft Entra
Search Properties	What Tab: • Subsystem | Microsoft 365 • Subsystem | Microsoft Entra
Searches Page	Built-in Reports: • All reports that include the events in the Microsoft 365 Exchange Online, Microsoft 365 SharePoint Online, Microsoft 365 OneDrive for Business, and Microsoft Entra facilities.
Alert Custom Email Dialog Exchange Online only.	Add Owners of Non-Owner Events option — to send an alert to the Exchange Mailbox owner when another user accesses their mailbox.

Deployment requirements

To successfully audit and report on events, ensure that your environment meets the minimum system requirements and you have reviewed the deployment information.

- System requirements
- License requirements
- Auditing and agent considerations

- Auditing in synchronized environments
- Upgrading Change Auditor

System requirements

For information about system requirements, see the Change Auditor Release Notes. For details on installing Change Auditor, see the Change Auditor Installation Guide.

License requirements

Change Auditor stops collecting events if a license expires. After you apply a license, the agent collects available events from the tenant that were missed. The Microsoft 365 and Microsoft Entra events are retained in the tenant for a specific period depending on your subscription type. If this period elapses before a new license is applied, some events are lost.

NOTE: Change Auditor now has a Change Auditor Government Cloud license available that enables the creation of Microsoft Entra ID and Microsoft 365 auditing templates specifically for GCC and GCC High tenants. However, it does not include auditing capabilities on its own. To audit specific services, you must also have the appropriate Change Auditor license types:

- Entra ID directory auditing requires the Change Auditor for Active Directory license.
- Entra ID sign-on and risk auditing requires the Change Auditor for Logon Activity User license.
- Microsoft 365 Exchange Online auditing requires the Change Auditor for Exchange license.
- Microsoft 365 SharePoint Online and OneDrive auditing requires the Change Auditor for SharePoint license.

NOTE: To verify that it is licensed, right-click the coordinator icon in the system tray and select **Licensing.**

Auditing and agent considerations

When auditing Microsoft 365 and Microsoft Entra ID, keep the following in mind:

- Occasionally duplicate auditing events are produced. This can occur when a service disruption requires that Microsoft administrators replay database transaction files to ensure that no events are lost. Change Auditor removes duplicated events that come in at the same time, but if an event that has already been sent to our database is sent again from Microsoft 365 it is displayed as a duplicate.
- By default. auditing settings that have been previously configured in the tenant for Exchange Online by third-party software are overwritten by the auditing setting specified in the Microsoft 365 template when the configuration is applied. You can, however, select to not overwrite the tenant settings.
- Change Auditor collects Microsoft's audit logs, and as a result the events and details reported are limited to what these logs provide.
- Change Auditor checks for new Microsoft Entra events every 15 minutes and for new Microsoft 365 events every 5 minutes.
- You can create multiple Microsoft Entra or Microsoft 365 templates to monitor multiple tenants; however, you must select a different agent for each template. A single agent cannot monitor multiple tenants. A single agent can audit both Microsoft Entra ID and Microsoft 365 against the same tenant.
- If your organization uses a proxy server to connect to the internet, you must configure the Proxy Server settings on the Agent Configuration page to audit Microsoft Entra and Microsoft 365 targets.

- The following URLs must be accessible for cloud auditing to be fully functional:

Commercial	GCC
https://login.microsoftonline.com	https://login.microsoftonline.com
https://graph.microsoft.com	https://graph.microsoft.com
https://outlook.office365.com	https://outlook.office365.com
https://manage.office.com	https://manage-gcc.office.com

Auditing in synchronized environments

Microsoft allows you to map identities between on-premises applications and cloud services. This is done by synchronizing your on-premises directories with Microsoft Entra ID using a Microsoft synchronization tool. When auditing Microsoft 365 or Microsoft Entra ID in this synchronized environment, Change Auditor provides extra event details by mapping identities.

The following conditions must be met for Change Auditor to perform the mapping:

- Synchronization performed with Microsoft Entra Connect.
- Microsoft Entra Connect synchronization process is active in your on-premises environment and directory sync is active in your cloud environment.
- Microsoft 365 or Microsoft Entra auditing template has been created to audit your online environment that is being synchronized with the on-premises Active Directory.
- The agent that is specified in the auditing template must be a member server of the forest being synchronized with Microsoft Entra ID.

NOTE: When synchronizing multiple forests into a single tenant, Change Auditor only provides additional information for the identities in the forest where an agent performing the Microsoft 365 auditing is installed.

When Federation with AD FS is used as the single sign-on method, Microsoft Entra logon events will no longer be generated since the authentication is done by the on-premises AD FS instance.

Upgrading Change Auditor

As of Change Auditor 7.2.0, Microsoft Entra and Microsoft 365 auditing templates will require MSAL (Microsoft Authentication Library) for authentication. New templates will no longer support basic authentication. Also, certificate authentication will now be required for web applications associated with Microsoft 365 auditing templates. See Managing Microsoft 365 templates for details.

When you upgrade from Change Auditor version 7.0.3 or earlier:

- Microsoft Graph API permissions must be applied on the web application associated with any existing Microsoft Entra and Microsoft 365 auditing templates for auditing to continue. For the list of required permissions see Edit a Microsoft Entra auditing template and Edit a Microsoft 365 auditing template.

  To apply the updated permissions, edit any existing templates and select the option to create a new web application to associate with it. The new web application will be created with the required permissions and auditing will continue.

  NOTE: Alternately, you can update the existing web application associated with the template by adding the required permissions directly on the web application in the Microsoft Entra admin center. See Edit a Microsoft Entra auditing template and Edit a Microsoft 365 auditing template for the list of required permissions. Once the permissions have been updated, restart the agent service for the new permissions to be applied immediately and auditing will continue.

When you upgrade from Change Auditor version 6.9.0 or earlier:

- Previously created Exchange Online auditing templates are deleted and will no longer display in the client.
- Agents previously assigned to audit Exchange Online stop auditing the Microsoft 365 Exchange Online tenant.

NOTE: You can still search and report on previously captured events. All legacy events are shown in either the Microsoft 365 Exchange Online Mailbox facility or the Microsoft 365 Exchange Online Administration facility.

- The Shared\Built-In\Exchange Online search folder is only available if it contained previously created Exchange Online custom searches.
- To capture sign-in risk events, you need to create a new template and select the Sign-ins option. These events are not captured automatically by an existing Microsoft Entra template.

To capture new events with Microsoft 365 and avoid losing any audited activities, after an upgrade:

1. Upgrade existing agents to the latest version.
2. Create an Microsoft 365 auditing template and configure Exchange Online auditing.

2

Configuring Microsoft 365 and Microsoft Entra ID auditing

- Managing Microsoft 365 templates
- Managing Microsoft Entra templates
- Considerations

Managing Microsoft 365 templates

Change Auditor audits activity for Exchange Online, SharePoint Online, and OneDrive for Business that corresponds to the events in the Microsoft 365 Security & Compliance Center unified audit log. Change Auditor allows you to easily track, report, and create alerts on activities such as:

- When Exchange Online mailboxes are created, deleted, and accessed.
- Permission changes to see which users are granted access to a mailbox.
- Mailbox activity by non-owner such as messages sent, read, deleted, and folders deleted
- Mailbox activity by owner for sensitive and high value mailboxes.
- When files and folders are accessed, created, deleted, uploaded, moved, renamed, and checked in and out of SharePoint Online and OneDrive for Business sites.

NOTE:

- Due to enhanced security measures, basic authentication is no longer supported for Microsoft 365 auditing; certificate authentication is now required.
- If you have existing Microsoft 365 auditing templates, the web application associated with them must be updated or replaced to support certificate authentication. See Edit a Microsoft 365 auditing template and for details.

For a compete list of events, their description, and default severity see the Change Auditor Microsoft 365 and Microsoft Entra ID Event Reference Guide.

Microsoft 365 auditing page

The Microsoft 365 auditing page contains a list of auditing templates that define the Microsoft 365 services and Exchange Online mailboxes to audit. The page displays when you select **Microsoft 365** from the Auditing task list in the navigation pane of the Administration Tasks page.

NOTE: Authorization to use the administration tasks on the Administrations Tasks tab is defined using the Application User Interface page under the Configuration task list. If you are denied access to the tasks on this page, see the Change Auditor User Guide for more information about how to gain access.

The following information is displayed for each template:

Template

Displays the name assigned to the auditing template when it was created. This name is the same as your tenant initial domain name.

Tenant Type

Displays whether the tenant is Commercial, GCC, or GCC High.

Status

Indicates whether the auditing template is enabled or disabled.

Administrative Events

Indicates whether Microsoft 365 Exchange Online administrative events are monitored.

Non-Owner Events

Indicates whether Microsoft 365 Exchange Online mailboxes are monitored for activities performed by users other than the mailbox owner.

SharePoint

Indicates whether SharePoint Online events are monitored.

OneDrive

Indicates whether OneDrive for Business events are monitored.

Overwrite Tenant Mailbox Auditing

Indicates whether the template auditing settings will overwrite the existing tenant auditing.

Create an Microsoft 365 auditing template

The following section describes the steps to create a template and the required web application so you can begin to audit the Microsoft 365 activity.

NOTE:

- Microsoft 365 Exchange, SharePoint and OneDrive auditing templates created in the Windows client defaults to 7 days (168 hours) of historical event collection. Historical event collection includes only mailbox auditing types previously enabled.
- Due to enhanced security measures, basic authentication is no longer supported for Microsoft 365 auditing; certificate authentication is now required.

  If you choose to create the required web application when you create the template, you can select to generate a self-signed certificate (default) or use a valid certificate from your personal certificate store. This will result in a properly configured web application.

  For a certificate to be valid, it must contain a private key that is marked as exportable, and must support client and server authentication.

  If you choose to use an existing web application when you create a template, you will need to specify the application ID, application key, and a valid certificate. For required configuration, see Using an existing web application.
- A Change Auditor Government Cloud license is required to create Microsoft Entra ID and Microsoft 365 auditing templates specifically for GCC and GCC High tenants.

To create a template

1. Open the Administration Tasks page.
2. Click **Auditing**.
3. Select **Micosoft 365** (under Applications).
4. Click **Add** to open the auditing wizard.
5. Under Authentication Configuration, select to **Create a new web application** or **Use existing web application**.

   If you select to create a new web application:

   a. Select the tenant type (Commercial, GCC, or GCC High.)

   b. Enter the **Microsoft Entra Directory Name.**

   c. Select **Generate self-signed certificate** or **Select certificate** to choose a previously created certificate from your personal store. By default, invalid certificates are filtered out from the list of available certificates.

   If you select to use an existing web application:

   a. Select the tenant type (Commercial, GCC, or GCC High.)

   b. Enter the **Microsoft Entra Directory Name, Application ID, Application key**, and select a previously created Application Certificate. For required settings and permissions, see Using an

existing web application and Microsoft documentation for details on integrating applications with Microsoft Entra ID, creating a web application, and adding a certificate to a web application.

6 Select the Microsoft 365 services to audit.

7 Click **Select agent** to view available agents and whether they are assigned to an Microsoft 365 auditing template. The Microsoft 365 cell contains 'None' if an agent is not assigned to a template, or 'Auditing' if it is assigned to a template. From this list, select the agent to capture the events and click **OK**.

NOTE:

- The agent must be upgraded to version 7.2 for certificate authentication support.
- PowerShell 5.1 or later is required.
- You cannot use an agent that is already assigned for Microsoft 365 auditing.
- GCC tenants are not supported on agents versions lower than version 7.5.

IMPORTANT: See the Change Auditor Release Notes for ports that must be opened on the agent server.

8 If you have selected to audit Exchange Online, you now need to choose the activities to audit. Click **Next**. For mailbox activity, you have the option to set mailbox auditing settings or use the settings that have been configured in the Exchange Online tenant.

NOTE: When you add and remove individual mailboxes for auditing or select to enable or disable owner auditing, the changes to the template are saved immediately. They are effective after the agent configuration is updated.

Available auditing events	Description
All administrative events	All changes made by administrators to the Microsoft 365 Exchange Online organization.
Set tenant mailbox auditing settings **NOTE:** When Change Auditor creates a template with default settings, it turns on mailbox non-owner activity auditing settings for every mailbox in your tenant. When you disable this option: • Mailbox non-owner activity auditing settings for every mailbox in your tenant are disabled as well. • Only the mailboxes specifically added to the template through your selection are audited. This may affect other systems that rely on having auditing enabled. **NOTE:** If you change the mailbox display name, email address, or UPN for a mailbox currently in a template, the auditing of the mailbox continues; however, the old mailbox settings display in the Change Auditor template. To see the new values, remove the mailbox and add it again.	By default, only activities performed by users other than the mailbox owner (non-owner activity) are audited. You can however, disable this option and audit only specific mailboxes. **NOTE:** Before you can select to audit individual mailboxes or update the configuration to audit owner events, select Finish to create the template. ***To add and remove individual mailboxes:*** 1 Click **Select mailboxes**. 2 To add a mailbox: a Enter the first letter or letters of the display name (not the mailbox name) in the top search field and click **Search**. b Select the appropriate entry from the mailbox results and click **Add**. 3 To remove a mailbox a Enter the first letter or letters of the display name (not the mailbox name) into the bottom search field and click **Search**. b Select the appropriate entry from the lower mailbox window and click **Remove**. You can refine your mailbox search by selecting Non-Owner Only, Owner, or All. (Owner includes mailboxes enabled for both owner and non-owner activity.)
	To optionally add owner auditing on specific mailboxes, enable the **Include Owner Activity** option. The "Owner Activity" audited on a configured mailbox include folder, message, and login events. **IMPORTANT:** Quest recommends that you select owner auditing for critical mailboxes only. Owner auditing for many mailboxes produces many events that may affect performance. ***To add or remove owner auditing on specific mailboxes:*** 1 Enter the first letter or letters of the display name (not the mailbox name) into the bottom search field and click Search. 2 Locate the required mailbox to enable or disable to **Include Owner Activity** as required. You can refine your mailbox search by selecting Non-Owner Only, Owner, or All. (Owner includes mailboxes enabled for both owner and non-owner activity.)
Use existing tenant mailbox settings	When this is enabled, the template settings will have no effect on the mailbox auditing settings. The settings in the tenant will be used.

9 Click **Next** to optionally specify the generic events to exclude from auditing based on their operations. The operations are visible in the "Activity Name/Operation" column of the Microsoft 365 built-in searches.

Generic events are dynamically created when associated activity is detected that does not have a corresponding event defined in Change Auditor. See Working with generic Microsoft 365 and Microsoft Entra events for more information.

10 Click **Finish**.

NOTE:

- The template name will be automatically set to your tenant initial domain name.
- When the agent's configuration is updated, it may take some time (approximately 1 second per mailbox) for it to be applied and the auditing to start after a template is created or modified.

11 Login to register Change Auditor in the tenant and ensure the required consent has been granted.

NOTE: The Microsoft sign-in page opens automatically once you have selected all your template settings and clicked **Finish**.

To grant permission for all administrators to create a web application:

1 Select an account with the Global Administrator role.

2 Enter the required password, and select **Sign in**.

3 Review the required permissions for the Change Auditor Configuration Assistant on the consent page.

To apply the consent to all the users in your organization, click to enable **Consent on behalf of your organization** and click **Accept**.

To apply the consent for just the current signed-in user simply click **Accept**.

NOTE: Consent is only required once per tenant. You may, however, be prompted to enter your log on credentials when creating a new web application.

Edit a Microsoft 365 auditing template

This section describes the steps to add or remove an Microsoft 365 service to audit and update the mailboxes and type of Exchange Online events to monitor.

To select a new agent, you must create a new template or use the Set-CAO365Template command through PowerShell. (See the Change Auditor PowerShell Command Guide for details.)

NOTE:

- Due to enhanced security measures, basic authentication is no longer supported for Microsoft 365 auditing; certificate authentication is now required.
- If you select to use an existing web application, it must be updated or replaced to support certificate authentication. See Using an existing web application for details.

To edit a template

1 Open the Administration Tasks page.

2 Click **Auditing**.

3 Select **Microsoft 365** (under Applications).

4 Select the template and click **Edit** to open the auditing wizard.

5 Under Authentication Configuration, select to **Create a new web application** or **Use existing web application**.

If you select to create a new web application, select **Generate self-signed certificate** or **Select certificate** to choose a previously created certificate from your personal store. By default, invalid certificates are filtered out from the list of available certificates.

If you select to use an existing web application, enter the **Application ID**, **Application Key**, and select a previously created Application Certificate. For required settings and permissions, see Using an existing

web application and Microsoft documentation for details on integrating applications with Microsoft Entra ID, creating a web application, and adding a certificate to a web application.

6 Add and remove the services to audit as required. Choose between Exchange Online, SharePoint Online, and OneDrive for Business.

NOTE: When you remove a service, the agent stops auditing its activity. If you later enable auditing, you cannot access events generated when auditing was disabled.

7 If you are auditing Exchange Online, click **Next** to update the events to audit.

Table 2. Available activities to audit

Available auditing events	Description
All administrative events	All changes made by administrators to the Exchange Online organization.
Set tenant mailbox auditing settings **NOTE:** When you add and remove individual mailboxes for auditing or select to enable or disable owner auditing, the changes to the template are saved immediately. They are effective after the agent configuration is updated. **NOTE:** When Change Auditor creates a template with default settings, it turns on mailbox non-owner activity auditing settings for every mailbox in your tenant. When you disable this option: • Mailbox non-owner activity auditing settings for every mailbox in your tenant are disabled as well. • Only the mailboxes specifically added to the template through your selection are audited. This may affect other systems that rely on having auditing enabled. **NOTE:** If you change the mailbox display name, email address, or UPN for a mailbox currently in a template, the auditing of the mailbox continues; however, the old mailbox settings display in the Change Auditor template. To see the new values, remove the mailbox and add it again.	By default, only activities performed by users other than the mailbox owner (non-owner activity) are audited. You can however, disable this option and audit only specific mailboxes. **NOTE:** Before you can select to audit individual mailboxes or update the configuration to audit owner events, select Finish to create the template. ***To add and remove individual mailboxes:*** 1 Click **Select mailboxes**. 2 To add a mailbox: a Enter the first letter or letters of the display name (not the mailbox name) in the top search field and click **Search**. b Select the appropriate entry from the mailbox results and click **Add**. 3 To remove a mailbox a Enter the first letter or letters of the display name (not the mailbox name) into the bottom search field and click **Search**. b Select the appropriate entry from the lower mailbox window and click **Remove**. You can refine your mailbox search by selecting Non-Owner Only, Owner, or All. (Owner includes mailboxes enabled for both owner and non-owner activity.)

Table 2. Available activities to audit

Available auditing events	Description
	To optionally add owner auditing on specific mailboxes, enable the **Include Owner Activity** option. The "Owner Activity" audited on a configured mailbox include folder, message, and login events. **IMPORTANT:** Quest recommends that you select owner auditing for critical mailboxes only. Owner auditing for many mailboxes produces many events that may affect performance. ***To add or remove owner auditing on specific mailboxes:*** 1 Enter the first letter or letters of the display name (not the mailbox name) into the bottom search field and click Search. 2 Locate the required mailbox to enable or disable to **Include Owner Activity** as required. You can refine your mailbox search by selecting Non-Owner Only, Owner, or All. (Owner includes mailboxes enabled for both owner and non-owner activity.)
Use existing tenant mailbox settings	When this is enabled, the template settings will have no effect on the mailbox auditing settings. The settings in the tenant will be used.

8 Click **Close**.

9 Click **Next** to optionally specify the generic events to exclude from auditing based on their operations. The operations are visible in the "Activity Name/Operation" column of the Microsoft 365 built-in searches. Generic events are dynamically created when associated activity is detected that does not have a corresponding event defined in Change Auditor.

10 Click **Finish** to apply the updates. When the agent's configuration is updated, it may take some time (approximately 1 second per mailbox) for it to be applied and the auditing to start after a template is created or modified.

11 You will need to login to register Change Auditor in the tenant and ensure the required consent has been granted. Note: Internet access is required.

NOTE: The Microsoft sign-in page opens automatically once you have selected all your template settings and clicked **Finish**.

To grant permission for all administrators to create a web application:

1 Select an account with the Global Administrator role.

2 Enter the required password, and select **Sign in**.

3 Review the required permissions for the Change Auditor Configuration Assistant on the consent page.

To apply the consent to all the users in your organization, click to enable **Consent on behalf of your organization** and click **Accept**.

To apply the consent for just the current signed-in user simply click **Accept**.

NOTE: Consent is only required once per tenant. You may, however, be prompted to enter your log on credentials when creating a new web application.

Using an existing web application

When you create or edit an Microsoft 365 auditing template and you select to use an existing web application it must be configured to support certificate authentication.

NOTE:

- The Microsoft Entra web application should be a single-tenant application.
- A redirect URI is not required.

To ensure that you will be able to audit mailbox activity:

- Upload the certificate for the web application through the Microsoft Entra admin center using **App Registration | All Applications | (web application) | Certificates & secrets | Certificate | Upload certificate**. The format for the certificate must be binary x.509 (.cer).
- Add the web application to the Exchange Administrator role for the tenant.
  1. In the Microsoft Entra admin center, select **Roles and Administrators | All roles.**
  2. Locate and open the **Exchange administrator** role.
  3. Select Add Assignments.
  4. Select **No members selected** under **Select Member(s)**.
  5. Select the required Application (client) ID guid.
  6. Save the new member with the **Select** button and then click **Next.**
  7. Change the Assignment Type to **Active**, ensure the **Permanently assigned** option is selected and enter a **Justification** (required).
  8. Click **Assign** to save the changes and verify that the web application name appears in the Members list for the Exchange Administrator role.

  NOTE: Must have a Client Secret configured in the web application "Certificates and Secrets" page.

- Ensure the required permissions are applied.

  NOTE: When creating a web application in the Microsoft Entra admin center, you are required to provide the following URLs: Sign-On URL, App ID URL. Specify any URL address that is unique to your tenant (for example: http://ChangeAuditorApp) for each of them.

  Once the following permissions are assigned to the web application, click **Grant admin consent for** and confirm with **Yes**.

  Microsoft Graph Application Permissions:

  - AuditLog.Read.All – Application - Read all audit log data
  - Directory.Read.All – Application - Read directory data
  - IdentityRiskEvent.Read.All – Application - Read all identity risk information

  Office 365 Management APIs

  Application Permissions:

  - ActivityFeed.Read – Application - Read activity data for your organization

  Office 365 Exchange Online

  Application Permissions:

  - Exchange.ManageApp - Application - Manage Exchange As Application

  See Microsoft documentation on assigning API permissions to applications for more details.

Disable a template

Disabling a template temporarily stops auditing activities without having to remove the template.

NOTE: Change Auditor stops collecting events if a license expired, the template is disabled, or the agent stops. After you apply a valid license, enable the template, or restart the agent Change Auditor collects available events from the tenant that were missed.

To disable a template

1. On the Microsoft 365 Auditing page, use one of the following methods to disable an auditing template:
   - Place your cursor in the **Status** cell for the auditing template to disable, click the arrow control, and select **Disabled**.
   - Right-click the template to disable and select **Disable**

   The entry in the **Status** column for the template changes to 'Disabled'.
2. To re-enable the auditing template, use the **Enable** option in either the **Status** cell or right-click menu.

Delete a template

NOTE: When you delete a template, the web application created in Microsoft Entra ID remains. You can delete the web application using the Microsoft Entra admin center.

To delete a template

1. On the Microsoft 365 Auditing page, select the template to delete and choose **Delete | Delete Template**.
2. Click **Yes** to confirm.

NOTE: Change Auditor now has a Change Auditor Government Cloud license available that enables the creation of Microsoft Entra ID and Microsoft 365 auditing templates specifically for GCC and GCC High tenants. However, it does not include auditing capabilities on its own. To audit specific services, you must also have the appropriate Change Auditor license types:

- Microsoft 365 Exchange Online auditing requires the Change Auditor for Exchange license.
- Microsoft 365 SharePoint Online and OneDrive auditing requires the Change Auditor for SharePoint license.

- Microsoft 365 Exchange, SharePoint and OneDrive auditing templates created in the Windows client defaults to 7 days (168 hours) of historical event collection. Historical event collection includes only mailbox auditing types previously enabled.
- Due to enhanced security measures, basic authentication is no longer supported for Microsoft 365 auditing; certificate authentication is now required.

  If you choose to create the required web application when you create the template, you can select to generate a self-signed certificate (default) or use a valid certificate from your personal certificate store. This will result in a properly configured web application.

  For a certificate to be valid, it must contain a private key that is marked as exportable, and must support client and server authentication.

  If you choose to use an existing web application when you create a template, you will need to specify the application ID, application key, and a valid certificate. For required configuration, see Using an existing web application.

Managing Microsoft Entra templates

Change Auditor for Active Directory simplifies the audit process by tracking, auditing, reporting, and alerting on activity in Microsoft Entra ID that impact your environment. Change Auditor correlates activity across the on-premises and cloud directories, providing you a single pane-of-glass view of your hybrid Active Directory environment and making it easy to search all events regardless of where they occurred.

You can 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 activity that corresponds to the events in the Microsoft Entra audit logs, sign-in activity report, and risky sign-ins report.

For a list of events, their description, and default severity see the Change Auditor Microsoft 365 and Microsoft Entra ID Event Reference Guide.

Microsoft Entra auditing page

The Microsoft Entra auditing page contains a list of auditing templates that define the directory to audit. The page displays when you select **Microsoft Entra** from the Auditing task list in the navigation pane of the Administration Tasks page.

NOTE: Authorization to use the administration tasks on the Administrations Tasks tab is defined using the Application User Interface page under the Configuration task list. If you are denied access to the tasks on this page, see the Change Auditor User Guide for more information about how to gain access.

The following information is displayed for each template:

Template

Displays the name assigned to the auditing template when it was created. This name is the same as your tenant initial domain name.

Tenant Type

Displays whether the tenant is Commercial, GCC, or GCC High.

Status

Indicates whether the auditing template is enabled or disabled.

Enabled templates that are lacking the required permissions for auditing are identified with a warning icon and a status of “Requires update”.

Audit Logs

Indicates whether the Microsoft Entra audit logs are monitored.

Sign-ins

Indicates whether Microsoft Entra sign-in and sign-in risk events are monitored.

Create a Microsoft Entra auditing template

The following section describes how to create a template and the required web application so you can begin to audit the Microsoft Entra ID activity. After the template is created, Change Auditor starts collecting events that are available on your tenant.

NOTE:

- You can only create one Microsoft Entra template per tenant.
- A Change Auditor Government Cloud license is required to create Microsoft Entra ID and Microsoft 365 auditing templates specifically for GCC and GCC High tenants.

To create an auditing template

1. Open the Administration Tasks page.
2. Click **Auditing**.
3. Select **Microsoft Entra** (under Directories).
4. Click **Add** to open the auditing wizard.
5. Under Authentication Configuration, select to **Create a new web application** or **Use existing web application**.

   If you select to create a new web application:

   a. Select the tenant type (Commercial, GCC, or GCC High.)

   b. Enter the **Microsoft Entra Directory Name**.

   If you select to create a new web application, you will need to login to register Change Auditor in the tenant and ensure the required consent has been granted. Note: Internet access is required.

   NOTE: The Microsoft sign-in page opens automatically once you have selected all your template settings and clicked **Finish**.

   To grant permission for all administrators to create a web application:

   1. Select an account with the Global Administrator role.
   2. Enter the required password, and select **Sign in**.
   3. Review the required permissions for the Change Auditor Configuration Assistant on the consent page.

      To apply the consent to all the users in your organization, click to enable **Consent on behalf of your organization** and click **Accept**.

      To apply the consent for just the current signed-in user simply click **Accept**.

   NOTE: Consent is only required once per tenant. You may, however, be prompted to enter your log on credentials when creating a new web application.

   If you select to use an existing web application:

   a. Select the tenant type (Commercial, GCC, or GCC High.)

b Enter the **Microsoft Entra Directory Name, Application ID,** and **Application key**. See Microsoft documentation for details on integrating applications with Microsoft Entra ID and creating a web application.

NOTE: The Microsoft Entra web application:

- Should be a single-tenant application. A redirect URI is not required.
- Must have a Client Secret configured in the web application "Certificates and Secrets" page.

Ensure the following permissions are assigned to the web application:

Microsoft Graph application permissions:

- AuditLog.Read.All – Application - Read all audit log data
- Directory.Read.All – Application - Read directory data
- IdentityRiskEvent.Read.All – Application - Read all identity risk information

If the app will also be used for Microsoft 365 templates, ensure that the following permissions are also set:

Office 365 Management APIs application permissions:

- ActivityFeed.Read – Application - Read activity data for your organization

Office 365 Exchange Online APIs application permissions:

- Exchange.ManageAsApp - Application - Manage Exchange As Application

For required configuration, see Using an existing web application.

Once the required permissions are applied, click **Grant admin consent for**… and confirm with **Yes**.

6 Select the activity to audit:

Audit Logs: Audits Microsoft Entra user, group, application, and directory activity. A Change Auditor for Active Directory license is required.

Sign-ins: Audits Microsoft Entra user sign-in and sign-in risk event activity. A Change Auditor for Logon Activity User license is required.

7 Click **Select agent** to view available agents and whether they are assigned to an auditing template. The Microsoft Entra cell contains 'None' if an agent is not assigned to a template, or 'Auditing' if it is assigned to a template. From this list, select the agent to capture the events and click **OK**.

NOTE:

- You cannot use an agent that is already assigned for Microsoft Entra ID auditing.
- GCC tenants are not supported on agents versions lower than version 7.5.
- See the Change Auditor Release Notes for ports that must be opened on the agent server.

8 Click **Finish** to create the template.

Edit a Microsoft Entra auditing template

This section describes how to add or remove Microsoft Entra activity to audit.

To select a new agent, you must create a new template or use the Set-CAAzureADTemplate command through PowerShell. (See the Change Auditor PowerShell Command Guide for details.)

To edit an auditing template

1 Open the Administration Tasks page.

2 Click **Auditing** button.

3 Select **Microsoft Entra** (under Directories).

4 Select the template and click **Edit** to open the auditing wizard.

5 Under Authentication Configuration, select to **Create a new web application** or **Use existing web application**.

If you select to create a new web application, you will need to login to register Change Auditor in the tenant and ensure the required consent has been granted. Note: Internet access is required.

NOTE: The Microsoft sign-in page opens automatically once you have selected all your template settings and clicked **Finish**.

To grant permission for all administrators to create a web application:

1. Select an account with the Global Administrator role.
2. Enter the required password, and select **Sign in**.
3. Review the required permissions for the Change Auditor Configuration Assistant on the consent page.

   To apply the consent to all the users in your organization, click to enable **Consent on behalf of your organization** and click **Accept**.

   To apply the consent for just the current signed-in user simply click **Accept**.

NOTE: Consent is only required once per tenant. You may, however, be prompted to enter your log on credentials when creating a new web application.

If you select to use an existing web application, enter the **Application ID** and **Application key**. See Microsoft documentation for details on integrating applications with Microsoft Entra ID and creating a web application.

NOTE: The Microsoft Entra web application:

- Should be a single-tenant application. A redirect URI is not required.
- Must have a Client Secret configured in the web application "Certificates and Secrets" page.

Ensure the following permissions are assigned to the web application:

Microsoft Graph application permissions:

- AuditLog.Read.All – Application - Read all audit log data
- Directory.Read.All – Application - Read directory data
- IdentityRiskEvent.Read.All – Application - Read all identity risk information

If the app will also be used for Microsoft 365 templates, ensure that the following permissions are also set:

Office 365 Management APIs application permissions:

- ActivityFeed.Read – Application - Read activity data for your organization

Office 365 Exchange Online APIs application permissions:

- Exchange.ManageAsApp - Application - Manage Exchange As Application

For required configuration, see Using an existing web application.

Once the required permissions are applied, click **Grant admin consent for**… and confirm with **Yes**.

6 Add and remove the activity to audit as required.

- **Audit Logs** audits Microsoft Entra user, group, application, and directory activity. A Change Auditor for Active Directory license is required.
- **Sign-ins**: Audits Microsoft Entra user sign-in and sign-in risk event activity. A Change Auditor for Logon Activity User license is required.

7 Click **Finish** to apply the updates.

Disable a template

Disabling a template temporarily stops auditing activities without having to remove the template.

NOTE: Change Auditor stops collecting events if a license expired, the template is disabled, or the agent stops. After you apply a valid license, enable the template, or restart the agent Change Auditor collects available events from the tenant that were missed.

To disable a template

1. On the Microsoft Entra Auditing page, use one of the following methods to disable an auditing template:
   - Place your cursor in the **Status** cell for the auditing template to disable, click the arrow control, and select **Disabled**.
   - Right-click the template to disable and select **Disable**

   The entry in the **Status** column for the template changes to 'Disabled'.
2. To re-enable the auditing template, use the **Enable** option in either the **Status** cell or right-click menu.

Delete a template

NOTE: When you delete a template, the web application created in Microsoft Entra ID remains. You can delete the web application using the Microsoft Entra admin center.

To delete a template

1. On the Microsoft Entra Auditing page, select the template to delete and choose **Delete | Delete Template**.
2. Click **Yes** to confirm.

Considerations

- If you have a synchronized environment, you may be auditing high volume synchronization events which have low value. To improve performance and reduce the number of events stored in the database, consider excluding some events with an excluded account template that targets the synchronization account and high volume Microsoft Entra events. Alternatively, you can select to purge the events after a specified number of days. If you set up a purge job for these events, ensure to configure the purge settings to delete the events before they are subject to any archival settings.
- Ensure that the appropriate Change Auditor licenses have been applied on all coordinators. See License requirements for license requirements.
- Ensure that the appropriate Microsoft Entra ID license has been applied:
  - To audit sign-in events, a Microsoft Entra ID P1 license is required.
  - To audit risk events, a Microsoft Entra ID P2 license is required.
- Ensure that the correct permissions have been applied on the web application that is associated with your template.
- Because Change Auditor collects Microsoft's audit logs, the events and details reported are limited to what these logs provide. If an event appears to be missing in Change Auditor, log onto the respective portal and review the audit logs to see if the event is listed.
  - For Microsoft Entra ID activity check the Audit Logs under Monitoring | Audit logs or go to https://portal.azure.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/Audit.
  - For Microsoft Entra Sign-ins check the Sign-ins under Monitoring | Sign-ins or go to https://aad.portal.azure.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/SignIns

- For Microsoft Entra risky sign-ins check the Risky sign-ins under Manage | Security | Risky sign-ins or go to https://aad.portal.azure.com/#blade/Microsoft_AAD_IAM/SecurityMenuBlade/RiskySignIns.
- For Microsoft 365 activity check the Audit Log under Search | Audit log search or go to https://protection.office.com/unifiedauditlog.

- See if the following internal events, which are in place to monitor the status of Microsoft Entra and Microsoft 365 auditing, have been generated. Persistent suspension of the auditing where auditing does not resume may lead to delayed event processing that requires administrator attention.
  - Microsoft Entra auditing has suspended

    Event generated when auditing is active, and then client or server HTTP error codes (4xx or 5xx *) are returned by the Microsoft Entra auditing service.
  - Microsoft Entra auditing has resumed

    Event generated when auditing was in a suspended state, and then a successful HTTP code is returned by the Microsoft Entra auditing service.
  - Microsoft 365 auditing has suspended

    Event generated when auditing is active, and then client or server HTTP error codes (4xx or 5xx *) are returned by the Microsoft 365 auditing service.
  - Microsoft 365 auditing has resumed

    Event generated when Microsoft 365 auditing was in a suspended state, and then a successful HTTP code is returned by the Microsoft 365 auditing service.

NOTE: Change Auditor now has a Change Auditor Government Cloud license available that enables the creation of Microsoft Entra ID and Microsoft 365 auditing templates specifically for GCC and GCC High tenants. However, it does not include auditing capabilities on its own. To audit specific services, you must also have the appropriate Change Auditor license types:

- Entra ID directory auditing requires the Change Auditor for Active Directory license.
- Entra ID sign-on and risk auditing requires the Change Auditor for Logon Activity User license.

3

Reports and Searches

- Introduction to Microsoft 365 and Microsoft Entra ID reporting
- Microsoft 365 built-in reports
- Custom searches
- Additional information for synchronized environments
- Working with generic Microsoft 365 and Microsoft Entra events
- Additional Microsoft 365 and Microsoft Entra event details

Introduction to Microsoft 365 and Microsoft Entra ID reporting

Change Auditor delivers both preconfigured and customizable reports displaying events in one centralized viewer. You can create custom search definitions to locate changes made in Microsoft 365 and Microsoft Entra ID. Using the available search properties across the bottom of the Searches page, you can define the search criteria and include specific columns to access more tenant details.

When Change Auditor is deployed in a synchronized environment, you can add extra columns to display extra mapping information about synchronized Active Directory users and their cloud identities for Microsoft 365 and Microsoft Entra events. For details, see Auditing in synchronized environments.

Microsoft 365 built-in reports

To see a complete list of built-in reports, see the Change Auditor Built-in Reports Reference Guide.

To view all Microsoft 365 searches:

1. Start the client and open the Searches tab.
2. In the explorer view (left pane), expand the **Shared | Built-in | Microsoft 365** folder.
3. Locate and double-click the required search in the right pane.

Microsoft Entra built-in reports

To see a complete list of built-in reports, see the Change Auditor Built-in Reports Reference Guide.

To view all Microsoft Entra searches:

1. Start the client and open the Searches tab.
2. In the explorer view (left pane), expand the **Shared | Built-in | Microsoft Entra** folder.
3. Locate and double-click the required search in the right pane.

Custom searches

You can create custom searches to meet your specific needs by using the following search properties tabs to define the criteria:

- What - allows you to search for events generated in a specific subsystem
- Who - allows you to search for events generated by a specific user
- Where - allows you to search for events captured by a specific agent
- When - allows you to search for events that occurred within a specific date and time range

NOTE: Selecting the **Private** folder creates a search that only you can run and view, whereas selecting the **Shared** folder creates a search that all users can view and run.

The following examples show how to use searches to find the information you need.

- Creating custom Exchange Online searches
- Creating a custom SharePoint Online and OneDrive for Business search
- Creating custom Microsoft Entra searches

Creating custom Exchange Online searches

To create a custom Exchange Online search:

1. Open the Searches page.
2. In the Explorer View, expand and select the folder where you want to save your search.
3. Click **New** to enable the Search Properties tabs across the bottom of the Searches page.
4. On the Info tab, enter a name and description for the search.
5. On the What tab, expand **Add** and click **Subsystem | Microsoft 365.**

   NOTE: You can use **Add with Events | Subsystem | Microsoft 365** (instead of **Add | Subsystem | Microsoft 365**) to search for events associated with an online mailbox or administrative action that already has an event associated with it.

6. Choose the **Selected Events** option to configure the search.

   NOTE: When multiple entries are added to the selection list at the bottom of the page, Change Auditor uses the 'OR' operator to evaluate events, returning events that meet any of the entries listed.

7. Select the **Mailbox Event** option.

Search	Procedure
To search for activities performed on a specific mailbox	1 Select **Mailbox Name** to specify the mailbox to include. 2 Select the comparison operator to use: **Contains** or **Does Not Contain**. Enter the pattern (character string) to be used to search for a match. For example: Contains admin finds all events for mailboxes that contain 'admin' anywhere in their name. 3 Click **Add** to add the expression to the selection list at the bottom of the page. Repeat this process to add any additional mailboxes to the search query.
To search for all activities performed on a specific folder and its contents across all monitored mailboxes	1 Select **Folder Name** to specify the folder to include. 2 Select the comparison operator to use: **Contains** or **Does Not Contain**. Enter the pattern (character string) to be used to search for a match. For example: Contains Inbox finds all events in 'Inbox' folder across all audited mailboxes. 3 Click **Add** to add the expression to the selection list at the bottom of the page. Repeat this process to add any additional folders to the search query.

Search	Procedure
To search for all activities by specific synchronized accounts based on their on-premises account name	1 Select **On-Premises User Name** to specify the user to include. 2 Select the comparison operator to use: **Like** or **Not Like**. Enter the pattern (character string and * wildcard character) to be used to search for a match. For example: Like *admin* finds all events performed by accounts that were synchronized from on-premises Active Directory that contain 'admin' anywhere in their sAMAccountName attribute. 3 Click **Add** to add the expression to the selection list. Repeat this process to add any additional users to the search query. **NOTE:** For this search to function, the Microsoft Entra ID must have been synchronized with the on-premises environment using Microsoft Entra Connect. For details, see Auditing in synchronized environments.
To search for all activities performed on synchronized mailboxes based on their on-premises account name	1 Select **On-Premises Target Name** to specify the user to include. Use this format domain\username. 2 Select the comparison operator to use: **Like** or **Not Like**. Enter the pattern (character string and * wildcard character) to be used to search for a match. For example: Like *admin* finds all events performed on synchronized mailboxes that have 'admin' anywhere in their on-premises sAMAccountName attribute. 3 Click **Add** to add the expression to the selection list. Repeat this process to add any additional mailboxes to the search query. **NOTE:** For this search to function, the Microsoft Entra ID must have been synchronized with the on-premises environment using Microsoft Entra Connect. For details, see Auditing in synchronized environments.
To search for activities performed on specific mailboxes based on their mailbox display name	1 Select **Target Display Name** to specify the mailbox to include. 2 Select the comparison operator to use: **Like** or **Not Like**. Enter the pattern (character string and * wildcard character) to be used to search for a match. For example: Like *admin* finds all events for mailboxes that contain 'admin' anywhere in their mailbox display name. 3 Click **Add** to add the expression to the selection list. Repeat this process to add any additional mailboxes to the search query.
To search for activities performed on specific mailboxes based on their synchronization status	1 Select **Target Sync Type** to specify the type of mailbox accounts to include based on how they are synchronized. 2 Select **In cloud** to include mailboxes existing only in the cloud. 3 Select **Synced from AD** to include mailboxes that have been synchronized from on-premises Active Directory. 4 Click **Add** to add the expression to the selection list.

To search for Administration cmdlets that were run:

1 On the What tab, expand **Add** and click **Subsystem | Microsoft 365.**

2 On the Microsoft 365 Exchange Online dialog, choose the **Selected Events** option to configure the search.

a Select the **Administration Cmdlet Event** option.

- Click **Cmdlet Name** and select the comparison operator to use: **Contains** or **Does not contain.** Enter the 'command' to use to search for a match. For example, to search for any 'add' users, enter add.
- Click **Cmdlet Parameters** select the comparison operator to use (**Contains** or **Does not contain**), and enter the name (or partial name) of a parameter to use to search for a match.
- Click **Parameter Values** select the comparison operator to use (**Contains** or **Does not contain**), and enter the value to use to search for a match.
- Click **Cmdlet Object**, select the comparison operator to use (**Contains** or **Does not contain**), and enter the name (or partial name) of a mailbox to use to search for a match.

NOTE:

- If the Cmdlet Name, Cmdlet Parameters, Parameter Values and Cmdlet Object are specified, all expressions must be met before an event is returned
- Cmdlet Parameters and Parameter Values can be searched separately; however, when both are selected the query is limited to the parameter that contains the selected value.

b To add the expression to the selection list, click **Add**.

c Repeat this process to add any additional search query requirements.

NOTE: When multiple entries are added to the selection list at the bottom of the page, Change Auditor uses the 'OR' operator to evaluate events, returning events that meet any of the entries listed.

Creating a custom SharePoint Online and OneDrive for Business search

To create a custom SharePoint Online and OneDrive for Business search:

1 Open the Searches page.

2 In the explorer view (left pane), expand and select the folder where you want to save your search.

3 Click **New** to enable the Search Properties tabs across the bottom of the Searches page.

4 On the Info tab, enter a name and description for the search.

5 On the What tab, expand **Add** and click **Subsystem | Microsoft 365.**

6 Choose the **Selected Events** option to configure the search.

7 Select **SharePoint/OneDrive Events**.

8 Select a service from the Microsoft 365 services filter to include in the search. You can choose SharePoint Online, OneDrive for Business, or both. If no additional filters are set, all events for the selected services are returned. You can specify additional filters as follows:

- Select the Operation filter to specify the operation to include in the search. Select a comparison operator (**Like** or **Not like**) and enter an operation name (character string and the * wildcard character). For example: Like *delete* will search for events where Operation contains 'delete'. For a list of all available operations, see the Microsoft support article "Search the audit log in the Microsoft 365 Security & Compliance Center".
- Select Site URL filter to specify the full or partial URL to include in the search. Select a comparison operator (**Like** or **Not like**) and enter a string (character string and the * wildcard character).
- Select the Target filter to specify the full or partial name of the operation target (for example, the folder, file, user, or group) to include in the search. Select a comparison operator (**Like** or **Not like**) and enter a string (character string and the * wildcard character). This search field corresponds to the contents of the Object Name column in the results grid.

9 Click **Add** to add the expression to the selection list.

10 Repeat this process to add any additional conditions to the search query.

NOTE: When multiple entries are added to the selection list at the bottom of the page, Change Auditor uses the 'OR' operator to evaluate events, returning events that meet any of the entries listed.

Displaying additional SharePoint Online and OneDrive for Business information

When auditing Microsoft 365, you can add columns to display extra SharePoint Online and OneDrive for Business information through the search Layout tab:

Table 4. Available columns

Layout Tab	Search Column Name	Description
Microsoft Entra - Microsoft 365 Site URL	Site Url	The SharePoint Online or OneDrive for Business website URL.
Microsoft Entra- Activity Name/Operation	Activity Name/Operation	This field matches Operation property in the Microsoft 365 Audit log.

Creating custom Microsoft Entra searches

To create a custom search for all Microsoft Entra events:

1 Open the Searches page.

2 In the explorer view (left pane), expand and select the folder where you want to save your search.

3 Click **New** to enable the Search Properties tabs across the bottom of the Searches page.

4 On the **Info** tab, enter a name and description for the search.

5 On the **What** tab, expand **Add** and click **Subsystem | Microsoft Entra.**

NOTE: You can use **Add with Events | Subsystem | Microsoft Entra** to select an existing event from the database and use its properties as a filter for a new search.

6 Select **All Events**.

7 Select the **Layout** tab and choose the Microsoft Entra information to include.

8 Click **OK** to save your selection and close the dialog.

After you have defined the search criteria, you can either save the search definition or run the search.

- To save the search definition without running it, click **Save**.
- To save and run the search, click **Run**.

To create a custom search for Microsoft Entra events based on facility or event:

1 Open the Searches page.

2 In the explorer view, expand and select the folder where you want to save your search.

3 Click **New** to enable the Search Properties tabs across the bottom of the Searches page.

4 On the **Info** tab, enter a name and description for the search.

5 On the **What** tab, expand **Add**. Select **Event Class.**

6 Group by the **Facility** column.

- To add all events within a facility, select the required Microsoft Entra facility, click **Add | Add All Events in Facility**, and click **OK**.

OR

- To add a specific event, select the required event class, click **Add | Add This Event**, and click **OK**.

7 Select the **Layout** tab and choose the Microsoft Entra ID information to include.

8 After you have defined the search criteria, you can either save the search definition or run the search.

- To save the search definition without running it, click **Save**.
- To save and run the search, click **Run**.

To create a custom search for Microsoft Entra events based on specific filter options:

1 Open the Searches page.

2 In the explorer view (left pane), expand and select the folder where you want to save your search.

3 Click **New** to enable the Search Properties tabs across the bottom of the Searches page.

4 On the Info tab, enter a name and description for the search.

5 On the What tab, expand **Add** and click **Subsystem | Microsoft Entra.**

> **NOTE:** You can use **Add with Events | Subsystem | Microsoft Entra** to select an existing event from the database and use its properties as a filter for a new search.

6 Select **Selected Events** to configure the search.

- Select the Category filter to specify the event category to include in the search. Select a comparison operator (**Like** or **Not like**) and enter a category name. For example, if you are interested only in activities related to self-service password resets, you would choose the “Self-service Password Management” category.
- Select the Activity Type filter to specify the activity to include in the search. Select a comparison operator (**Like** or **Not like**) and enter an activity type. For example, to only show user related activities you would select “User” as the activity type.
- Select the Activity Name filter to specify the activity to include in the search. (For sign-in risk events, this will show the detected activity that occurred on the risk event.) Select a comparison operator (**Like** or **Not like**) and enter an activity name (character string and the * wildcard character). For example: Like *delete* will search for events where Activity contains ‘delete’.
- Select the Activity Details filter to include activity details in the search. (For sign-in risk events use the status of the risk event, such as Resolved). Select a comparison operator (**Like** or **Not like**) and enter a full or partial string (character string and the * wildcard character). For example, the 'Self-serve password reset flow activity progress' activity provides several different details including: User started the mobile SMS verification option, User started the e-mail verification option, or User successfully reset password. You can leave this filter blank to return events for all activities or narrow the search based on the activity details.
- Select the Target filter to specify the target (primary and secondary targets) to include in the search. (For sign-in risk events, the field searches for the risk event type such as Sign-in from anonymous IP address). Select a comparison operator (**Like** or **Not like**) and enter a full or partial name (character string and the * wildcard character). The Target filter searches across the following properties: Object Name (Cloud Target Name), Target Display Name, On-Premises Target, Subject Name, Subject Display Name, and On-Premises Subject.

  > **NOTE:** When Microsoft Entra events include multiple targets, Change Auditor identifies these as Target (primary target) and Subject (secondary target).

- Select the Location filter to specify the country, state, or city to include in the search. Select a comparison operator (**Like** or **Not like**) and enter a full or partial name (character string and the * wildcard character).
- Select the Activity Origin filter to specify the activity origin to include in the search. You can choose between Cloud (event activity was performed directly in the cloud) or AD (event activity was originally performed on-premises and was synchronized to the cloud).

- Select the Sync Type filter to specify the target (primary and secondary targets) synchronization type to include in the search. You can choose between In Cloud (target object exists only in the cloud) and Synced from AD (target object was synchronized from Active Directory).

  NOTE: When Microsoft Entra events include multiple targets, Change Auditor identifies these as Target (primary target) and Subject (secondary target).

7. Click **Add** to add the expression to the selection list.
8. Repeat this process to add any additional expressions to the search query.

   NOTE: When multiple entries are added to the selection list at the bottom of the page, Change Auditor uses the 'OR' operator to evaluate events, returning events that meet any of the entries listed.

9. Select the **Layout** tab and choose the Microsoft Entra ID information to include.
10. After you have defined the search criteria, you can either save the search definition or run the search.
    - To save the search definition without running it, click **Save**.
    - To save and run the search, click **Run**.

Displaying additional Microsoft Entra information

When auditing Microsoft Entra ID, you can add columns to display extra information through the search Layout tab:

Table 5. Available columns

Layout Tab	Search Column Name	Description
Microsoft Entra - Activity Type	Activity Type	The activity resource type.
Microsoft Entra - Activity Name/Operation	Activity Name/Operation	The activity that was performed as part of the event.
Microsoft Entra - Activity Details	Activity Details	Additional information about audited activity. For example, for 'Self-serve password reset flow activity progress' it shows what step the user is performing. For sign-in risk events, this shows the status of the risk event, such as "Closed (resolved)".
Microsoft Entra - Category	Category	The activity category, such as Terms of use, Core Directory, Application Proxy, Account Provisioning, Invited Users, etc.
Microsoft Entra - Sign-in City	City	The city from which the user signed in or attempted to sign in to an application.
Microsoft Entra - Sign-in State	State	The state from which the user signed in or attempted to sign in to an application.
Microsoft Entra - Sign-in Country	Country	The country from which the user signed in or attempted to sign in to an application.

NOTE: The sign-in columns are only applicable to Microsoft Entra sign in and sign in risk events.

NOTE: For Microsoft Entra sign in events the time detected in the search results references the sign in time.

Additional information for synchronized environments

When auditing Microsoft 365 and Microsoft Entra ID in a synchronized environment, you can add columns to display extra mapping information through the search Layout tab:

Table 6. Available columns

Layout Tab	Search Column Name	Description
Microsoft Entra - Activity Origin	Activity Origin	‘Cloud’ indicates that the event activity was performed directly in the cloud. ‘AD’ indicates that the event activity was originally performed on-premises and was synchronized to the cloud.
Microsoft Entra - On-premises User	On-premises User	Domain and sAMAccountName of the on-premises user that corresponds to the cloud user that initiated the event.
Microsoft Entra - On-premises Target	On-premises Target	Domain and sAMAccountName of the on-premises object that corresponds to the cloud object that was the target of the event.
Microsoft Entra - Target Sync Type	Target Sync Type	‘In Cloud’ indicates that the target object exists only in the cloud ‘Synced from AD’ indicates that the target object was synchronized from Active Directory.
Microsoft Entra - Target Display Name	Target Display Name	Display the on-premises object display name for synchronized environments or the cloud object display name only for cloud-only objects.
Microsoft Entra - Tenant Initial Domain	Tenant Initial Domain	Default Microsoft Entra domain name.
Microsoft Entra - Tenant Display Name	Tenant Display Name	Tenant display name.
Microsoft Entra - Subject Sync Type	Subject Sync Type	‘SyncedFromAD’ indicates that the subject object was synchronized from Active Directory. ‘In Cloud’ indicates that the subject object exists only in the cloud.
Microsoft Entra - Subject Display Name	Subject Display Name	Displays the Active Directory on-premises name if a hybrid object and the Microsoft Entra name if a cloud object.
Microsoft Entra - On-premises Subject	On-premises Subject	Domain and sAMAccountName of the on-premises object that corresponds to the cloud object that was the subject of the event.
Subject Name	Subject Name	Microsoft Entra object name regardless of whether a cloud or hybrid object.

In addition to the search columns, the ‘Who’ field shows the mapping information in the event details pane. In cloud only deployments, this field displays the cloud user that initiated the event. If it is a synchronized deployment, the associated on-premises user is displayed after the cloud user in square brackets.

Working with generic Microsoft 365 and Microsoft Entra events

The Microsoft Entra ID audit reports and the Microsoft 365 audit logs are continuously evolving. To ensure that Change Auditor is synchronized with these updates, generic events have been introduced. Each Microsoft Entra and Microsoft 365 facility in Change Auditor has one generic event defined.

The generic event is generated each time an activity occurs that does not have a corresponding event defined in Change Auditor. For example, “Microsoft Entra- User event” is generated when activities such as “Reset password (self-service)” or “Unlock user account” are performed in Microsoft Entra ID. Activity information is populated in additional columns and the description for the event (What statement) is dynamically constructed based upon the activity and target object name.

When working with these events, you can add additional columns to the search layout to view information about the activity.

Table 7. Available columns

Layout Tab	Search Column Name	Description
Microsoft Entra - Activity Name/Operation	Activity Name/Operation	Represents the activity that was performed as part of the event. For sign-in risk events, this shows the risk event type.
Microsoft Entra - Activity Details	Activity Details	Provides additional information about audited activity. For example: • For ‘Self-serve password reset flow activity progress’, it shows what step the user is performing. • For sign-in events it shows why the sign-in failed. • For sign-in risk events, this shows the risk event status.

For a complete list of the activities available see Microsoft documentation on “Audit activity reports” and “Search the audit log in the Microsoft 365 Security & Compliance Center”.

Additional Microsoft 365 and Microsoft Entra event details

The event details pane contains the following additional information to help gain a better understanding of the activities taking place in Microsoft 365 Exchange Online, SharePoint Online, OneDrive for Business, and Microsoft Entra ID.

Table 8. Event details

Tab	Available information
Overview	Displays a high-level view of the activity that is generated for each event. You can quickly see when the event occurred, who made the change, what changed, where the change originated, the activity, the target type, synchronization type, subject type, subject synchronization type, activity type, category, and action, Additional information for sign-in events include the reason for a sign-in failure and the sign-in location. Additional information for sign-in risk events include the type of risk activity, risk status, risk level, and origin (IP address).
Target (Microsoft Entra events only) **NOTE:** This tab is not displayed for sign-in and sign-in risk events.	Displays details on the property updates with the old and new value when available. It also displays information about multiple targets affected by a single event. For example, when a user added to a group, you can see both the user and the group as affected targets. When there are multiple targets, the target that best matches the activity type is displayed as the primary target in the Overview tab.
Details	Displays all available properties for a deeper analysis of the activity, including the raw data from the Microsoft Entra Reporting API. For sign-in risk events, it contains raw data from the Microsoft Entra Identity Protection API.
Parameters (Exchange Online Administration events only)	Displays the parameters used to run the Microsoft 365 Administrative command.
Item	Displays Id, rights, SID, Upn, name and path details for Exchange Online permission additions, removals, or modifications.
Additional Info (Microsoft Entra risky events only)	Displays risk event additional information such as user agent, related event time in UTC, related users agent, device information, related location, request ID, correlation ID.

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.