

Quest On Demand Audit

User 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 Web site (<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, TIP, MOBILE, or VIDEO:** An information icon indicates supporting information.

Contents

Introducing On Demand Audit	5
Quest On Demand Overview	5
Documentation Roadmap	5
Additional resources	6
Quest On Demand Audit Overview	6
Accessing Quest On Demand Audit	6
Configuring On Demand Audit	7
Working with tenants	7
Granting required consent	8
Configuring tenant auditing	8
Working with On Demand Audit	9
Using the dashboard	9
Searching for specific event data (Quick Search)	10
Working with searches	10
Running a search	11
Using built in searches	11
Creating a custom search	12
Copying an existing search	13
Creating a search from an existing search	13
Creating or filtering a search based on event details	14
Customizing the columns displayed in a search	14
Visualizing searches	15
Viewing search results and event details	15
Copying event details	16
Modifying a search	16
Deleting a search	17
Working with categories	17
Auditing Azure Active Directory	17
Event collection and Azure Active Directory subscription	18
Working with Azure Active Directory Searches	18
Working with Azure Active Directory events with multiple targets	19
Auditing risk events	20
Azure Active Directory built in searches	21
Auditing Office 365	21
Office 365 built in searches	22
Appendix A: Working with search columns and filters	23

Available search filters and columns	23
Available pre-defined filter values	25
About us	27
Contacting Quest	27
Technical support resources	27

Introducing On Demand Audit

- [Quest On Demand Overview](#)
- [Documentation Roadmap](#)
- [Quest On Demand Audit Overview](#)
- [Accessing Quest On Demand Audit](#)

Quest On Demand Overview

Quest On Demand is a Software as a Service (SaaS) application, available through quest-on-demand.com, that provides access to multiple Quest Software Microsoft management tools through a single interface.

On Demand management is based on the concepts of organizations, modules, and Azure Active Directory tenants. When you sign up for the On Demand service, you create an organization that can subscribe to modules. Organization administrators can use the tools provided by the On Demand modules to perform administrative actions on Azure Active Directory tenants.

Currently, the following modules are available:

- Audit
- Migration
- Recovery for Azure Active Directory
- Policy Management for Skype for Business Online
- Policy Management for Exchange Online

Documentation Roadmap

The On Demand Global Settings User Guide contains the documentation for tasks that apply to all On Demand modules. This includes:

- Signing up for Quest On Demand
- Managing Organizations and Regions
- Tenant Management
- Configuration settings (Permissions and subscription information)
- Audit logs

Each management module, such as On Demand Audit, contains its own user guide and release notes that contain the following module -specific content:

- The Release Notes contain a release history and details new features, resolved issues, and known issues.
- The User Guide contains descriptions and procedures for the tasks you can perform with the management tool.

Additional resources

- For sales or other inquiries, visit www.quest.com/contact.
- To sign up for a trial or purchase a subscription, go to <https://www.quest.com/on-demand>.
- 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 [Quest On Demand community](#) provides a space for blog posts and a forum to discuss the On Demand products.

Quest On Demand Audit Overview

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

On Demand Audit audits:

- Exchange Online, SharePoint Online, and OneDrive for Business activity that corresponds to the events in the Office 365 Security & Compliance Center unified audit log. See [Auditing Office 365](#) for details.
- Azure Active Directory user, group, application, and directory activity that corresponds to the events in the Azure Active Directory audit logs, sign-in activity report, and risky sign-ins report. See [Auditing Azure Active Directory](#) for details.

Accessing Quest On Demand Audit

To access On Demand Audit, you need to sign up for the Quest On Demand service and create an organization. For that, go to [Quest On Demand](#) and use one of the following options:

- Sign up using the existing Quest account.
- Create a new Quest account and sign up for Quest On Demand.
- Join an existing On Demand organization.

For details, see Signing up for Quest On Demand section in On Demand Global Settings User Guide.

Configuring On Demand Audit

- [Working with tenants](#)
- [Granting required consent](#)
- [Configuring tenant auditing](#)

Working with tenants

You must have a tenant in the organization to audit the Office 365 and Azure Active Directory activity.

i | **NOTE:** When you remove a tenant, event collection stops.
If you add the tenant back, you will need to select the services to audit again.

To add a tenant:

1. Log in to On Demand, select **Auditing**
2. Click **Start by Adding a Tenant** on the **Audit** module.
3. Click **Add tenant** and **OK**.
4. The Azure sign in page opens. Sign in as a Global administrator account for the tenant.
5. Read through the required permissions and select **Accept**. You are redirected to the list of tenants available in the Quest On Demand application.

To add more tenants, repeat steps 3 and 4.

Before you can audit the tenant, you need to grant On Demand Audit consent to audit its Office 365 and Azure Active Directory activity. See [Granting required consent](#)

Granting required consent

Before you can audit Office 365 and Azure Active Directory activity and generate searches, On Demand must be granted consent to audit the Office 365 organization and its tenants.

i **NOTE:** The Audit configuration page displays the status of the consent for the tenant:

- Need to grant admin consent - when consent is not granted.
- Admin consent granted - when consent is granted.

To grant the required consent:

1. Log in to On Demand, and select **Auditing**.
2. Click **Go** on the **Audit** module.
3. Click the **Need to grant admin consent** link. The Azure sign in page opens. If you are signed in as the Global administrator for the tenant, you can grant consent to the On Demand Audit application.
4. Read through the required permissions and select **Accept**. Once this is complete, you are redirected to On Demand Audit page.

Configuring tenant auditing

You need to configure tenant auditing by selecting the services to audit.

Once selected, the Audit homepage card displays the audited services with the number of events in the last hour.

i **NOTE:** You need to enable auditing of Office 365 mailboxes to audit Exchange Online. For more information, see [Microsoft documentation](#).

i **NOTE:** You can audit multiple tenants, and each can have a distinct auditing configuration. If a tenant is added to multiple On Demand organizations, the tenant auditing configuration is unique for each organization and events are collected and stored for each organization.

To configure auditing

1. Log in to On Demand, and select **Auditing**.
2. Click **Go** on the **Audit** module.
3. Select the services to audit. You can select to audit all, Exchange Online - Administrative activity, Exchange Online - Mailbox activity, SharePoint Online, OneDrive for Business, Azure Active Directory - Audit Logs, and Azure Active Directory - Sign-ins. (Azure Active Directory - Sign-ins includes risk events.)
4. Click **Save**.

The configuration is added to Azure and events will be collected for the selected services. The configuration is checked every 5 minutes to see which activities to add to the database.

i **NOTE:** If a service is disabled or consent is revoked, events collection stops. If auditing is re-enabled, events are collected from the last collected event (or last available event).

Working with On Demand Audit

- [Using the dashboard](#)
- [Searching for specific event data \(Quick Search\)](#)
- [Working with searches](#)
- [Auditing Azure Active Directory](#)
- [Auditing Office 365](#)

Using the dashboard

When you open On Demand Audit, the dashboard displays a visual summary of the most important metrics of the Office 365 and Azure Active Directory activity in your organization.

You can use the data to discover trends and quickly locate the information that you need. To further drill into the event details, you can use the visualizations offered with searches. See [Visualizing searches](#).

The information in the dashboard is updated in real time, allowing you to quickly gain valuable insights into the activity taking place in your organization.

The Overview tab displays:

- Number of events (Event count)
- Total number of unique users
- Activity (A drop-down is available so that you can select the activity that you want to see.)
- User Name (A drop-down is available so that you can select the users that you want to see.)
- Top 10 active users
- Activity heat map that visually breaks down the activity in a display that shows which events are more prevalent.

The Sign-ins tab displays:

- Sign-ins by location on a map
- Sign-ins by unique application and users or you can filter for specific applications and users

- Successful and failed sign-ins
- Sign in activity timeline

By hovering over the right corner of any section, you are provided with more options for sharing and customizing the data.

- Select Export data to .xlsx or .csv file.
- Sort the data
- Use the available slider to fine grain the dates included in the view.

You can also perform a broad search through all your events, using the Quick Search.

Searching for specific event data (Quick Search)

Performing a quick search allows you to search through all events based on a specific value, term, or keyword.

To search for data within an event

1. Enter the search term in the **Quick Search** box and click the magnifying glass icon.

The resulting lists display all events that have a value matching the search term or value, sorted by the time detected. The search terms are highlighted in the search results and event details to allow you to quickly scan for matches.

Working with searches

- [Running a search](#)
- [Using built in searches](#)
- [Creating a custom search](#)
- [Copying an existing search](#)
- [Creating a search from an existing search](#)
- [Creating or filtering a search based on event details](#)
- [Appendix A: Working with search columns and filters](#)
- [Customizing the columns displayed in a search](#)
- [Visualizing searches](#)
- [Viewing search results and event details](#)
- [Copying event details](#)
- [Modifying a search](#)
- [Deleting a search](#)
- [Working with categories](#)

Running a search

Once On Demand Audit captures an event, you can view all available event data through searches. You can use custom searches based on your own criteria or built in searches that are configured to meet the most common requests. See [Creating a custom search](#) and [Using built in searches](#).

i | **NOTE:** Custom user-built searches are identified by the following icon to the left of the search.

 New Search - Tue Mar 20 2018

To run a previously saved or built in search

1. Select the **Searches** tab.
2. Locate the required search in the list of categories.
3. To run the search, simply click it or highlight it and click the run (arrow) icon.

From here you can:

- Select an event to see all the event details.
- Modify the search (Custom user-built searches only). See [Modifying a search](#).
- Refresh the display.
- Visualize the event data. See [Visualizing searches](#)
- Select a column to sort the search results by column.
- Create a new search or filter the search based on a specific event detail. See [Creating or filtering a search based on event details](#).

Using built in searches

On Demand Audit provides predefined searches which allow you to quickly retrieve valuable configuration change information from various perspectives.

Although built in searches cannot be modified, you can create a new search based on it and customize the settings to suit your needs. See [Creating a search from an existing search](#).

The following built in searches are available:

- All Events category
 - All events in the past 24 hours
 - All events in the past 7 days
- Azure Active Directory (See [Azure Active Directory built in searches](#))
- Office 365 category (See [Office 365 built in searches](#))

To run a built in search

1. Select the **Searches** tab.
2. Locate the search in the required category - **All Events** or **Office 365**.
3. Highlight the search and click the arrow icon to run it.

From here you can:

- Select an event to see all the event details.
- Refresh the display.
- Visualize the event data. See [Visualizing searches](#)

Creating a custom search

Custom searches allow you to locate and report on the data that is of interest to you. The associated search preview updates as you construct a search to ensure you are getting the desired results. For options, see [Customizing the columns displayed in a search](#).

To create a search

1. Under the **Searches** tab, click **New Search**.
2. Enter a name for the search. By default, the new search will be created in the **My Searches** category. If required, select a different category.
3. Click **Add** to enter the required search criteria.
4. Select as many filters as required. Search terms are highlighted in the preview (and search results and event details) to allow you to quickly scan for matches.
5. Click **Edit Columns** to arrange, add, and remove the columns displayed in the search. See [Customizing the columns displayed in a search](#).

Available filters

The available string operators include:

- equals
- does not equal
- contains
- does not contain
- in
- not in
- starts with
- does not start with
- ends with
- does not end

The available integer operators for sign-in events:

- equals_number
- does_not_equal_number
- greater_than
- greater_than_or_equals
- less_than

- less_than_or_equals
- between_number

The available date and time operators include:

- during last number of days or hours (By default, this is set to the last 7 days for all new searches.)
- between
- before
- after

Copying an existing search

Copying an existing search allows you to take advantage of existing settings and modify as required.

1. Under the **Searches** tab, select the search.
2. Click the copy icon. The search is created with "Copy" appended to its name.
3. Enter a new name and change the category, if required, by selecting a new category from the drop down list.
4. Click **Copy**.

The new search is now available to edit as required.

Creating a search from an existing search

Creating a search based on an existing search allows you to add granularity by adjusting the filters, category, and columns to suit your specific needs.

To create a new search based on an existing custom or built in search

1. Under the **Searches** tab, select the search.
2. Click the pencil icon to modify the search.
3. Remove, add, edit search criteria as required. Search terms are highlighted in the preview (and search results and event details) to allow you to quickly scan for matches.
4. If required, click **Edit Columns** to rearrange, add, and remove columns. See [Customizing the columns displayed in a search](#).
5. Select **Save As**.
6. Edit the search name and select the category.
7. Click **Save**.

Creating or filtering a search based on event details

You can quickly create a new search or refine an existing search based on values within the event details pane. This allows you to delve deeper into the details found from existing searches.

To create a search based on an event detail

1. Select the **Searches** tab.
2. Locate the required search in the list of categories.
3. To run the search, simply click it or highlight it and click the run (arrow) icon.
4. Select the required value, click the More options icon (...), and select **New Search on this value**.
5. You can select to run the search, save it, or further filter it as required.

To filter a search based on an event detail

1. Select the **Searches** tab.
2. Locate the required search in the list of categories.
3. To run the search, simply click it or highlight it and click the run (arrow) icon.
4. Select the required value, click the More options icon (...), and select **Add filter on this value**.
5. You can select to run the search, save it, or further filter it as required.

Customizing the columns displayed in a search

When you create a search, a preview displays to help ensure the search criteria meet your needs. You can customize the columns that display in the generated report and easily rearrange the column display order through drag and drop.

The following columns are included by default:

- Time Detected
- User (Actor)
- Activity
- Target
- Origin IP
- Service
- Status (All Event searches and Sign-in searches only)
- Tenant Name

To rearrange, add, and remove the columns displayed in the search

1. As you create a search, click **Edit Columns**.
2. Drag and drop the columns to change the order.

3. To remove a column, click the **X** next to the appropriate column.
4. To add a column, click **Add Column**.
5. Save your changes.

For a list of available columns, see [Appendix A: Working with search columns and filters](#)

Visualizing searches

You can visualize saved searches to provide insights on the Office 365 events taking place in your organization and your Azure Active Directory.

The Overview tab displays:

- Number of events (Event count)
- Total number of unique users
- Activity (A drop-down is available so that you can select the activity that you want to see.)
- User Name (A drop-down is available so that you can select the users that you want to see.)
- Top 10 active users
- Activity heat map that visually breaks down the activity in a display that shows which events are more prevalent.

The Sign-ins tab displays:

- Sign-ins by location on a map
- Sign-ins by unique application and users or you can filter for specific applications and users
- Successful and failed sign-ins
- Sign in activity timeline

To see a visual representation of a search

1. Select the **Searches** tab, choose a search, and click the visualization (chart) icon. You can also click the run (arrow) icon, then click the **Visualize** button. (Note: This is only available for saved searches.)

By hovering over the right corner of any section, you are provided with more options for sharing and customizing the data that is presented.

- Select Export data to .xlsx or .csv file.
- Show the underlying data
- Sort the data
- Use the available slider to to fine grain the dates included in the view.

Viewing search results and event details

When you select an event that has been returned from a search, you can view all the details of the activity that triggered the event. If the search contains string filters, the string is highlighted in the search results and event details to allows you to quickly scan for matches.

To view event details

1. Select the **Searches** tab.
2. Locate the required search in the list of categories.
3. Highlight the search and click the arrow icon to run it.
4. Click an event to open a new window that contains all the event details.

Copying event details

When you select an event that has been returned from a search, you can the event details to a clipboard to paste in another application. If you select to copy all details, the formatting is retained.

To copy event details

1. Select the **Searches** tab.
2. Locate the required search in the list of categories.
3. Highlight the search and click the arrow icon to run it.
4. Click an event to open a new window that contains all the event details.
5. Select **Copy to clipboard** to copy all event details to a clipboard.

Modifying a search

Only custom searches can be modified.

i NOTE: Built in searches cannot be modified. However, you can create a new search based on it and customize the settings to suit your needs. See [Creating a search from an existing search](#).

To modify a search

1. Under the **Searches** tab, select the search.
2. Click the pencil icon to modify the search.
3. Edit the search name, remove, add, edit search criteria as required. Search terms are highlighted in the preview (and search results and event details) to allows you to quickly scan for matches.
4. Change the category, if required by selecting a new category from the drop don list.
5. Click **Edit Columns** to rearrange, add, and remove columns as required. See [Customizing the columns displayed in a search](#).
6. Click **Save** to apply the changes.

Deleting a search

To remove a search

1. Select the **Searches** tab.
2. Locate the required search in the list of categories.
3. Highlight the search and click the **X** icon to delete it.
4. Click **Delete** to confirm the removal.

Working with categories

By default, the following categories are available:

- **My searches:** New searches default to the "My Searches" category, unless another category is specified.
- **All:** All configured searches.
- **All Events:** All events in the last 24 hours and 7 days.
- **Azure Active Directory:** Azure Active Directory application, directory, group, role, self-service password, user created, user deleted, and user events in the last 7 days.
- **Office 365:** Office 365 and SharePoint online searches.

To create a category

1. Under the **Searches** tab, click **Add** in the Categories field.
2. Enter the category name and click **Add**.

To assign a search to a new category

1. Under the **Searches** tab, select the search.
2. Click the pencil icon to modify the search.
3. Drop down the **Category** field and select the required category.
4. Click **Save**.

To edit the name of a category

1. Under the **Searches** tab, select the category.
2. Highlight the category, and click the pencil icon to the left of the category.
3. Enter a new name for the category and click **Save**.

Auditing Azure Active Directory

On Demand Audit simplifies the audit process by tracking, auditing, and reporting on activity that corresponds to the events in the Azure Active Directory audit logs, sign-in activity report, and risky sign-ins report.

NOTE: An Azure Active Directory Premium license is required for On Demand Audit to audit sign-in and risky sign-in activity.

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.

For example, you can easily track and report on activities such as:

- When users and groups are added to and removed from the directory.
- When user and group attributes are changed.
- Successful and failed logins.
- Suspicious sign-in activity.

Event collection and Azure Active Directory subscription

Historical auditing is dependent on your Azure Active Directory subscription.

Subscription	On Demand AuditEvent Collection
Azure Active Directory license	Azure AD - Audit Log historical events in the last 7 days
Azure Active Directory premium license (Optional)	Azure AD - Audit Log historical events in the last 30 days
Azure Active Directory premium license (Required)	AzureAD - Sign-ins historical events in the last 30 days
Azure Active Directory premium license (Required)	AzureAD - Risky Sign-ins historical events in the last 30 days

Working with Azure Active Directory Searches

On Demand Audit provides numerous [Azure Active Directory built in searches](#) that allow you to locate and report on the Azure Active Directory data. If required, you can also easily create custom searches to locate specific information that is of interest to you.

There are numerous columns, filters, and pre-defined values that you can use to help you find the information you need to secure your environment.

See [Creating a custom search](#) and [Appendix A: Working with search columns and filters](#) for more details.

Azure Active Directory- specific columns

The following columns are available to display additional Azure Active Directory information:

Audit module	Columns
Azure Active Directory - Audit Log	<ul style="list-style-type: none">• Azure AD Activity Type• Azure AD Activity Operation Type• Azure AD Result Description• Azure AD Category

Audit module	Columns
Azure Active Directory Sign-ins	<ul style="list-style-type: none"> Error Code Failure Reason Location
Azure Active Directory Risky Sign-ins	<ul style="list-style-type: none"> RiskEventStatus RiskEventId RiskEventType RiskLevel RiskEventDateTime PreviousCity (impossible travel risk events only) PreviousState (impossible travel risk events only) PreviousCountry (impossible travel risk events only) PreviousSignInDateTime (impossible travel risk events only) PreviousIpAddress (impossible travel risk events only) PreviousLocation (impossible travel risk events only) RiskEventDetails MalwareName isAtypicalLocation

Working with Azure Active Directory events with multiple targets

To help filter searches and fine tune the results, the following Azure Active Directory group membership, group ownership, and role membership activity has been split so that a single event is reported based on the target and subject

Group Membership Event	Target	Subject
Add member to group	Group being modified	User or group added to a group
Add group membership	User or group added to a group	Group being modified
Remove member from group	Group from which a user or group is removed	User or group being removed from a group
Remove group membership	User or group being removed from a group	Group from which the user or group is removed
Add owner to group	Group that is modified	User added as group owner
Group ownership assigned	User added as group owner	Group that is modified

Group Membership Event	Target	Subject
Remove owner from group	Group that is modified as a result of a removed owner	User removed as group owner
Group ownership removed	User removed as group owner	Group that is modified as a result of a removed owner

Role Event	Target	Subject
Add member to role	Role to which a user is added	User added to the role
Role assignment added	User added to a role	Role to which a user is added
Remove member from role	Role from which a user is removed	User removed from a role
Role assignment removed	User removed from a role.	Role from which a user is removed
Add eligible member to role	Role to which a user is added	User added to a role
Role assignment added to eligible member	User added to a role	Role to which a user is added

Additional filters

You can, for example, create a search for all group membership events and see distinct events for both the group you are adding a user to and the user you are adding to the group. Using the target to filter your searches allows you to pinpoint the activity by specific users, and changes to critical groups and roles. See [Appendix A: Working with search columns and filters](#) for a complete list of available filters.

Auditing risk events

On Demand Audit captures both the risk event as well as when an administrator takes action on the detected risk.

i | **IMPORTANT:** To capture and view this information, ensure that you have enabled auditing of the Azure Active Directory - Audit Logs module.

This following information is listed in the Azure AD risk event's activity.:

- "New risk event detected" event when the Microsoft Azure Active Directory Identity Protection portal creates a new risk event.
- "Admin dismisses risk event", "Admin reactivates risk" event, and "Admin resolves risk" when the Microsoft audit logs creates an event for an administrator's actions.

Azure Active Directory built in searches

On Demand Audit provides the following Azure Active Directory built-in searches that are based on the most common and complex requests for information:

- Azure AD application events in the past 7 days
- Azure AD directory events in the past 7 days
- Azure AD events in the past 7 days
- Azure AD failed sign-in events in the past 7 days
- Azure AD group events in the past 7 days
- Azure AD group member changes in the past 7 days
- Azure AD group owner changes in the past 7 days
- Azure AD risk events in the past 7 days
- Azure AD role events in the past 7 days
- Azure AD role member changes in the past 7 days
- Azure AD self-service password management events in the past 7 days
- Azure AD sign-in events in the past 7 days
- Azure AD successful sign-in events in the past 7 days
- Azure AD tenant level configuration changes in the last 180 days
- Azure AD user created events in the past 7 days
- Azure AD user deleted events in the past 7 days
- Azure AD user events in the past 7 days
- Important changes for critical Azure AD directory roles in the past 7 days
- Objects added/removed from Azure AD groups in the past 7 days
- Objects added/removed from Azure AD roles in the past 7 days
- Users added/removed as owner of Azure AD groups in the past 7 days

See [Using built in searches](#) for details on running the searches and creating custom searches based off the built in searches.

Auditing Office 365

On Demand Audit audits activity for Exchange Online, SharePoint Online, and OneDrive for Business that corresponds to the events in the Office 365 Security & Compliance Center unified audit log.

You can easily track and identify important 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.

Office 365 built in searches

On Demand Audit provides the following Office 365 built-in searches that are based on the most common and complex requests for information

- Email forwarding enabled in the past 7 days
- Office 365 activity from ad-hoc external recipients in the past 7 days
- Office 365 events from EXT Users in the past 7 days
- Office 365 events in the past 7 days
- Office 365 Exchange Online administrative cmdlets executed in the past 7 days
- Office 365 Exchange Online events in the past 7 days
- Office 365 Exchange Online mailbox events in the past 7 days
- Office 365 Exchange Online mailbox login activity in the past 24 hours
- Office 365 Exchange Online mailbox non-owner activity in the past 7 days
- Office 365 OneDrive for Business events in the past 7 days
- Office 365 OneDrive for Business file activity events in the past 7 days
- Office 365 OneDrive for Business folder activity events in the past 7 days
- Office 365 SharePoint Online events in the past 7 days
- Office 365 SharePoint Online file activity events in the past 7 days
- Office 365 SharePoint Online folder activity events in the past 7
- OneDrive for Business and SharePoint Online anonymous link events in the past 180 days

See [Using built in searches](#) for details on running the searches and creating custom searches based off the built in searches.

Appendix A: Working with search columns and filters

The following columns, filters, and pre-defined values are available to help you locate the information you need to secure your environment.

Available search filters and columns

Filters and columns

- Activity
- Actor Name
- Actor Object Id
- Actor PUID
- Actor Service Principle Name
- ActorUserPrincipalName
- Additional Details
- Affected Items
- Application Id
- Application Name
- Atypical Location
- Audit Item
- Audit Source
- Azure AD Activity Operation Type
- Azure AD Activity Type
- Azure AD Category
- Azure AD Result Description
- City
- MFA Authentication Detail
- MFA Authentication Method
- MFA Required
- MFA Result
- Modified Object
- Modified Properties
- Object Id
- Office365 Organization Id
- Organization Id
- Organization Name
- Origin IP
- Originating Server
- Parameters
- Previous City
- Previous Country
- Previous IP
- Previous Sign-In Time
- Previous State
- Record Type
- Result Status

Filters and columns

- Client Info String
- Client IP Address
- Client Machine Name
- Client Process Name
- Client Version
- Correlation Id
- Country
- Cross-Mailbox Operations
- Custom Event
- Destination File Extension
- Destination FileName
- Destination Folder
- Destination MailboxId Id
- Destination MailboxId Owner
- Master Account Sid
- Destination MailboxId Owner Sid
- Destination MailboxId Owner UPN
- Destination relative URL
- Device Information
- Distribution Group Name
- Domain Name
- Error Code
- Event Data
- Event Id
- Event Source
- Event Version
- External Access
- Failure Reason
- Folder
- Internal Correlation Id
- Item type
- Logon User Sid
- Risk Event Details
- Risk Event Id
- Risk Event Time
- Risk Event Type
- Risk Level
- Schema Id
- Send as User Mailbox Guid
- Send as User SMTP
- Send on behalf of User Mailbox Guid
- Send on behalf of User SMTP
- Sharing Target
- Sharing Target Type
- Sharing Type
- Site
- Site Url
- Source File Extensions
- Source FileName
- Source Folders
- Source Name
- Source Relative Url
- State
- Status
- Subject
- Subject Name
- Subject Object Id
- Subject PUID
- Subject Resource Type
- Subject Service Principle Name
- Target
- Target Additional Details
- Target Name
- Target Object Id
- Target PUID
- Target Resource Type

Filters and columns

- Logon User Display Name
- Logon Type
- Malware Name
- Mailbox Owner UPN
- Mailbox Owner Sid
- Mailbox Owner Master Account Sid
- Mailbox Name
- Mailbox Guid
- Machine Id
- Machine Domain Info
- Target Service Principle Name
- Target Type
- Target User Principle Name
- Tenant Id
- Tenant Name
- Time Detected
- Time Received
- Url
- User (Actor)
- User Agent
- User Display Name
- User Id
- User Key
- User Shared With
- User Type

Available pre-defined filter values

Filter	Pre-defined values
Risk Event Status	<ul style="list-style-type: none">• Active• Closed (ignored)• Closed (marked as false positive)• Closed (MFA Auto-Closed)• Closed (Multiple Reasons)• Closed (resolved)• Login Blocked• Remediated
Risk Level	<ul style="list-style-type: none">• Low• Medium• High
Risk Event Type	<ul style="list-style-type: none">• Anonymous IP Risk Event• Impossible Travel Risk Event• Leaked Credentials Risk Event

Filter	Pre-defined values
Service	<ul style="list-style-type: none"> • Malware Risk Event • Suspicious IP Risk Event • Unfamiliar Location Risk Event
MFA Required	<ul style="list-style-type: none"> • Yes • No
Status	<ul style="list-style-type: none"> • Failed • Successful

Quest provides software solutions for the rapidly-changing world of enterprise IT. We help simplify the challenges caused by data explosion, cloud expansion, hybrid datacenters, security threats, and regulatory requirements. We are a global provider to 130,000 companies across 100 countries, including 95% of the Fortune 500 and 90% of the Global 1000. Since 1987, we have built a portfolio of solutions that now includes database management, data protection, identity and access management, Microsoft platform management, and unified endpoint management. With Quest, organizations spend less time on IT administration and more time on business innovation. 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