Quest

Quest On Demand Audit

User Guide

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.

On Demand Audit User Guide
Updated - Decmber 2019

Contents

Introducing 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
- Group Management
- Migration
- Policy Management for Skype for Business Online
- Policy Management for Exchange Online
- Recovery

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

Quest On Demand Audit 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.

3

Configuring On Demand Audit

Working with tenants

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

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.
2. From My Dashboard, click **Add tenant.**
3. Sign in as a Global administrator account for the tenant on the Azure sign in page.
4. Read through the required permissions and select **Accept**.
5. To add another tenant, navigate to the **Auditing** module. From the **Configuration** tab, click **Add tenant**. 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.

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.

NOTE: You need to enable auditing of Office 365 mailboxes to audit Exchange Online. For more information, see Microsoft documentation.

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.

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).

Adding a user to an organization

If you are the On Demand administrator or the owner of the On Demand Audit subscription, you can add users to an existing organization so they can access the audit data. If you are not the subscription owner or administrator, contact your On Demand administrator for access.

To add a user to an organization

1. Log in to On Demand, and select the required organization.
2. Select **Access Control | Users**.
3. Under **User Name**, enter the user's email address.
4. Under **Assigned Role**, select Auditing Administrator.
5. Click **Add User**.

Supported regions

A Microsoft Azure region is a set of datacenters deployed within a geographic area. Selecting the correct region for your On Demand organization enables you to achieve higher performance and supports your requirements and preferences regarding data location. Specifying the region for your organization determines the geographical region where your data is stored.

During sign up, you can choose the region where your On Demand data will be hosted. The following regions are currently supported for On Demand Audit:

- United States
- Europe

Change Auditor Integration

Integrating with Change Auditor, provides a single view of activity across hybrid Microsoft environments and turns on-premise events into rich visualizations to investigate incidents faster. Events sent to On Demand Audit include historical events gathered up to 30 days prior to upgrade to Change Auditor 7.0.0 (or higher). Availability of historical events is dependent on how long Change Auditor has been deployed in the environment.

To begin the integration, a connection between Change Auditor and your organization in On Demand Audit is configured in Change Auditor. Once the connection is made, Change Auditor will begin to send events.

- Registering a Change Auditor Installation
- Pausing Change Auditor event forwarding
- Resuming Change Auditor event forwarding
- Removing a Change Auditor Installation
- Reviewing the status of your Change Auditor installation
- Active Directory Built in searches

Registering a Change Auditor Installation

Change Auditor installations are configured through the Change Auditor client. Once an installation is registered, Change Auditor will begin sending event data.

NOTE: Once a configuration is in place, all coordinators which belong to the Change Auditor Installation will be registered with On Demand Audit.

NOTE: To create the configuration, you must use the account that created the On Demand subscription or an account that has been delegated the appropriate permissions from your On Demand administrator.

- If you do not own the On Demand subscription, you need to contact your On Demand administrator for access.
- If you are the On Demand administrator, you can delegate the required permissions by adding the required accounts to the Auditing Administrator role through the On Demand Access page. See Adding a user to an organization for details.

NOTE: Required URL access

To create a configuration with On Demand Audit, Change Auditor clients and coordinators must be able to access: https://quest-on-demand.com.

To send events to On Demand Audit, Change Auditorcoordinators must be able to access: https://odauditprod-wus297293-iot.azure-devices.net/

To create a configuration

1. From the Change Auditor client, select **View | Administration**.
2. Select **Configuration | On Demand Audit**.
3. Select **Sign in and Configure** to create the connection.

4. Enter your Quest account credentials to sign in to On Demand Audit.
5. Choose the required organization if prompted and click **Select Organization**.
6. By default, the current installation name is used for the configuration name. If required, you can enter a different name for the configuration. This is the configuration name used in On Demand Audit; it does not change the Change Auditor installation name.
7. Click **Finish**.

Pausing Change Auditor event forwarding

To pause the sending of Change Auditor events

1. Navigate to the **Auditing** module.
2. From the **Configuration** tab, select the ellipsis (...) on the Change Auditor tile and choose **Pause**.
3. Click **OK** to confirm.

Resuming Change Auditor event forwarding

To begin sending Change Auditor events for a paused installation

1. Navigate to the **Auditing** module.
2. From the **Configuration** tab, select the ellipsis (...) on the Change Auditor tile and choose **Resume Sending Events**.
3. Click **OK** to confirm.

Removing a Change Auditor Installation

When you remove a Change Auditor installation that is registered with On Demand Audit (or delete the associated organization), Change Auditor will stop sending events.

To remove a Change Auditor installation

1. Navigate to the **Auditing** module.
2. From the **Configuration** tab, select the ellipsis (...) on the Change Auditor tile and choose **Remove Installation**.
3. Click **OK** to confirm.

Reviewing the status of your Change Auditor installation

From the Configuration tab, you can quickly see the status of your Change Auditor installation.
The information includes:

- Installation status - whether it is connected, disconnected, or paused.
- The time of the last update.
- The number of connected coordinators.
- The installed version of Change Auditor.

NOTE: If the Change Auditor installation is disconnected, there may be an issue with the Change Auditor coordinators. The following steps may help reconnect the installation:

- Restart the coordinator to attempt to reconnect to On Demand Audit and check the coordinator logs for error messages. See Manage Change Auditor coordinators section in the Change Auditor User Guide for information on restarting the coordinator and accessing the logs.
- Search for the errors in the Change Auditor Knowledge Base: https://support.quest.com/change-auditor/kb.

If the installation is still disconnected, contact Customer Support.

Active Directory Built in searches

If you have a Change Auditor installation registered with On Demand Audit, you will have access to the following Active Directory built-in searches:

- AD all account lockout events in the past 7 days
- AD all attribute changes in the past 7 days
- AD all computer events in the past 7 days
- AD all domain controller events in the past 7 days
- AD all events in the past 24 hours
- AD all events in the past 7 days
- AD all events including ActiveRoles/GPOADmin initiator in the past 7 days
- AD all forest configuration events in the past 7 days
- AD all objects deleted in the past 7 days
- AD all OU events in the past 7 days
- AD all replication events in the past 7 days
- AD all schema configuration events in the past 7 days
- AD all security changes in the last 30 days
- AD all site events in the past 7 days

- AD all user events in the past 7 days
- AD computers added in the past 30 days
- AD computers disabled in the past 30 days
- AD computers enabled in the past 30 days
- AD computers moved in the past 30 days
- AD computers removed in the past 30 days
- AD computers renamed in the past 30 days
- AD critical group membership changes in the past 30 days
- AD group added in the past 30 days
- AD group deleted in the past 30 days
- AD group member added changes in the past 30 days
- AD group member removed changes in the past 30 days
- AD group moved in the past 30 days
- AD group nested member added changes in the past 30 days
- AD group nested member removed changes in the past 30 days
- AD group renamed in the past 30 days
- AD users added in the past 30 days
- AD users added to group in the past 30 days
- AD users deleted in the past 30 days
- AD users disabled in the past 30 days
- AD users enabled in the past 30 days
- AD users locked out in the past 30 days
- AD users moved in the past 30 days
- AD users removed from group in the past 30 days
- AD users renamed in the past 30 days
- AD users unlocked in the past 30 days

See Using built in searches for details on running the searches and creating custom searches based off the built in searches.

See Change Auditor Integration for details on adding on-premises event data to your On Demand Audit deployment.

4

Working with On Demand Audit

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 allows you to quickly scan for matches.

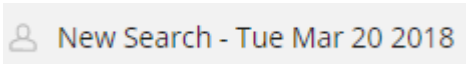
Working with searches

- 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.

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



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.
- Create and disable alerts. See Working with alerts and alert plans.

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
- Active Directory
- 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.
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
- Create an alert for the search. See Working with alerts and alert plans

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 allows 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.
6. Click **Save**.
7. If required, click **Alert**, select the required alert plan (or create a new alert plan) to notify the required individuals , click **Save**. See Working with alerts and alert plans

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 don 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 allows 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**.
8. If required, click **Alert**, select the required alert plan (or create a new alert plan) to notify the required individuals , click **Save**. See Working with alerts and alert plans

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 selecting 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 allow you to quickly scan for matches.

A summary of important event details is displayed at the top of the event details that includes:

- Activity Name
- Service
- Time Detected
- User display name
- Target
- Location
- Status (Successful/Failed)

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.
5. Click the **Event Link** to create a dedicated page for the event details within On Demand Audit. Once created you can view the information, copy the URL to share with others, or bookmark it for future use.

Copying event details

When selecting an event that has been returned from a search, you can copy the event details to clipboard to paste into another application.

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.

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.
7. If required, click **Alert**, select the required alert plan (or create a new alert plan) to notify the required individuals , click **Save**. See Working with alerts and alert plans

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**.

Working with alerts and alert plans

Alerts and their associated alert plans allow those responsible for the security of your environment to stay on top of changes and activities as they occur.

Through the Alerts page you can:

- View the number of alerts created in the last 24 hours for each search.
- View the number of associated alert plans.
- Enable and disable individual alerts.
- Remove alerts.
- Add and remove associated alert plans.
- Review searches that have alerts created for them.

By clicking on an alert you can:

- View and access all alert plans associated with alert.
- Edit the alert.
- View its associated search.

For details, see Managing alerts and alert plans

Managing alerts and alert plans

Creating an alert for a search allows those responsible for the security of your environment to receive detailed information about vital changes and activities as they occur.

The alert plan allows you to configure who will receive alerts so that they can take the appropriate action to address the outlined risks to your environment.

NOTE: You can select to assign any number of alert plans to an alert.

To create an alert with an associated alert plan

1. Under the **Searches** tab, select the search.
2. Click **Alert**.
3. Configure the alert plan to associate with the alert.

   To use an existing alert plan, select it and click **Save**.
   To create and enable a new alert plan, enter a name for it and click **Save**. Next, select the link to enter the email recipients for the alert, and click **Save**.

To edit an alert and associated alert plan

1. Under the **Alerts** tab, select **Alerts**.
2. Select the required alert, and click **Edit Alert**.
3. Add and remove the alert plans associate with the alert as required.

   To add existing alert plan, select it and click **Save**.

   To remove an existing alert plan, clear the check box , and click **Save**.

   To create and enable a new alert plan, enter a name for it and click **Save**. Next, select the link to enter the email recipients for the alert, and click **Save**.

To remove an alert

NOTE: The default alert plan cannot be removed.

1. Under the **Alerts** tab, select **Alerts**.
2. Select the required alert, and click the **X** icon to delete it.

To create an alert plan

1. Under the **Alerts** tab, select **Alert Plans**.
2. Click **New Plan**.
3. Enter a name for the alert plan and enter the required email address, and click **Save**.
4. Click **Send Test** and **OK** to verify that a test alert is sent to the appropriate recipients.

To rename an alert plan

NOTE: The default alert plan cannot be renamed.

1. Under the **Alerts** tab, select **Alert Plans**.
2. Select the required alert plan, click in the name field, rename as required, and click **Save**.

To remove an alert plan

1. Under the **Alerts** tab, select **Alert Plans**.
2. Select the required alert, and click the **X** icon to delete it.

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 (P1) license or higher 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	• Azure AD Activity Type • Azure AD Activity Operation Type • Azure AD Result Description • Azure AD Category
Azure Active Directory Sign-ins	• Error Code • Failure Reason • Location
Azure Active Directory Risky Sign-ins	• 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
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.

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	• Active • Closed (ignored) • Closed (marked as false positive) • Closed (MFA Auto-Closed) • Closed (Multiple Reasons) • Closed (resolved) • Login Blocked • Remediated
Risk Level	• Low • Medium • High
Risk Event Type	• Anonymous IP Risk Event • Impossible Travel Risk Event • Leaked Credentials Risk Event

Filter	Pre-defined values
	• Malware Risk Event • Suspicious IP Risk Event • Unfamiliar Location Risk Event
Service	• Azure Active Directory • Exchange • OneDrive • SharePoint
MFA Required	• Yes • No
Status	• Failed • Successful

About us

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