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

Legend

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

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

On Demand Audit User Guide
Updated - March 2018

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
- 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

On Demand Audit provides extensive auditing of critical activities and detailed reports about vital changes taking place in Microsoft Office 365 Exchange Online, SharePoint Online, and OneDrive for Business. Continually being in-the-know helps you to prove compliance, drive security, and improve up time while proactively auditing changes to configurations and permissions.

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 report 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.

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

You must have a tenant in the organization to audit the Office 365 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 **Audit**.
2. Click **Start by Adding a Tenant**.
3. Click **Add tenant** and **Continue.**
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.

   Before you can audit the tenant, you need to grant On Demand Audit consent to audit its Office 365 activity. See Granting required consent

Granting required consent

Before you can audit Office 365 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. Select **Audit** and click **Go**.
2. 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.
3. 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 Office 365 services to audit.

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, or OneDrive for Business.
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).

Working with On Demand Audit

- Using the dashboard
- Working with searches

Using the dashboard

When you open On Demand Audit, the dashboard displays a visual summary of the most important metrics of the Office 365 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 such as:

- Total number of events.
- Top 10 active users.
- A visual breakdown of the services where the events are generated with the available heatmap.
- Event time line.

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.

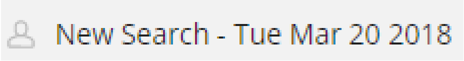
Working with searches

- Running a search
- Using built in searches

- Creating a custom search
- Customizing the columns displayed in a search
- Visualizing searches
- Viewing search results and 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 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.
>
> 
>
> 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. Highlight the search and click the arrow icon to run it.

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

Using built in searches

NOTE: Built in searches cannot be modified. But you can see the search criteria being applied by selecting the modify icon.

The following built-in searches are available:

- 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

To run a built in search

1. Select the **Searches** tab.
2. Locate the required search in the **Office 365** 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

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.
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
- starts with
- does not start with

- ends with
- does not end

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

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.

The following columns are included by default:

- Time Detected
- User (Actor)
- Activity
- Target
- Origin IP
- Service
- 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.

The available columns include:

- Affected Items
- Audit Item
- Client Info String
- Client IP Address
- Client Machine Name
- Client Process Name
- Client Version
- Mailbox Owner Sid
- Mailbox Owner UPN
- Modified Object
- Modified Properties
- Object Id
- Office365 Organization Id
- Organization Id

- 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
- Distribution Group Name
- Event Data
- Event Id
- Event Source
- External Access
- Folder
- Item type
- Logon Type
- Logon User Display Name
- Logon User Sid
- Machine Domain Info
- Machine Id
- Mailbox Guid
- Mailbox Name
- Mailbox Owner Master Account Sid
- Organization Name
- Originating Server
- Parameters
- Record Type
- Result Status
- 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
- Target Type
- Time Received
- Url
- User Agent

NOTE: For a description of the available columns see the Microsoft article Detailed properties in the Office 365 audit log.

Visualizing searches

You can visualize saved searches to provide insights on the Office 365 events taking place in your organization. The information displayed include:

- 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.

To see a visual representation of a search

1. Select the **Searches** tab, choose a search, and click the run (arrow) icon.
2. Click the **Visualize** button. (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.

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.

Modifying a 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.
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**.

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

New searches default to the My searches category, unless another category is specified.

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**.

About us

We are more than just a name

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

Our brand, our vision. Together.

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

Contacting Quest

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

Technical support resources

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

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

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