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
Last Updated - September 2020

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
- License Management
- Migration
- Recovery

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, Teams, 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, OneDrive for Busines, Teams, and SharePoint Online 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 in On Demand Global Settings User Guide.

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:

- Australia
- Canada
- Europe
- UK
- United States

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. You can select to audit:

- All service
- Audit Azure Active Directory - Audit Logs
- Azure Active Directory - Sign-ins. (Azure Active Directory - Sign-ins includes risk events.)
- Exchange Online - Administrative activity
- Exchange Online - Mailbox activity
- OneDrive for Business
- SharePoint Online
- Teams

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.
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).

Historical event collection

Historical event collection is dependent on the type of license that you are using:

NOTE: If you are currently auditing Office 365 services, any additional Office 365 service added at a later date will not have historical events gathered.

- For a trial license Azure Active Directory, Office 365, and Change Auditor historical event collection is restricted to the 24 hours before the service is added.
- When you change to a paid subscription, historical event collection is based on when the Office 365 and Azure Active Directory service is first enabled or the Change Auditor integration is configured.
  - Historical events are not collected for services that were enabled during a trial subscription.
  - Historical events are collected for services that were not enabled during the trial subscription period.
  - If you disable a service during a trial period, change to a paid subscription, and enable the service again historical events will not be collected

See the following table for historical event collection details:

Service	Changing from a trial license to a paid subscription
Office 365 • Exchange Admin activity • Mailbox activity • Sharepoint Online • OneDrive for Business • Teams	For services that were not enabled with a trial license, historical events are collected for past 7 days.
Azure Active Directory • Audit Logs • Sign-ins (and risk events)	For services that were not enabled with a trial license, historical events are collected for either 7 or 30 past days, depending on the Azure Active Directory report retention policies.

Service	Changing from a trial license to a paid subscription
Change Auditor • Active Directory • Group Policy • Logon Activity	For services that were not enabled with a trial license, historical events are collected based on what is configured in Change Auditor.

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.

When you add a user to an organization, you also assign one or more roles. The role assignment determines what permission level a user has and ultimately, what tasks the user can perform. Assigning roles and setting user permissions is referred to as access control. See On Demand Audit Access Control roles.

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 the required role.
5. Click **Add User**.

On Demand Audit Access Control roles

Each access control role has a specific set of permissions that determines what tasks a user assigned to the role can perform . Your Quest On Demand organization comes configured with a number of default roles. The default role permissions settings cannot be changed, but you can create custom roles with specific permission settings to align with your company policies. For more information, see Adding users to an organization in the On Demand Global Settings User Guide.

The following default roles are available to help you manage your security and compliance auditing with On Demand Audit:

- Audit Administrator role allows full access to On Demand Audit.
- Audit Operator role allows users to manage searches and create alerts.

Role	Permission Details
Audit Administrator	• Can manage alert plans (View and manage alert plans, including creation and deletion.) • Can manage alerts (View, manage, create, and delete alerts, view the list of alert plans including their detailed configuration.)

Role	Permission Details
	• Can export search results (Can export search results to a csv or csv.zip file.) • Can Manage Azure AD Tenant Configurations for Audit (View and modify the Office 365 and Azure Active Directory tenant configuration for On Demand Audit.) • Can Manage Change Auditor Installation Configuration (View and modify the configuration for Change Auditor installations that are connected to the organization. This includes adding and removing installations in the organization.) • Can manage private searches (Create and modify private searches and manage search categories.) • Can run private searches (Run and preview searches.) • Can run search visualization (Run a search visualization.) • Can run shared searches (Run and preview shared searches.) • Can view dashboard (View the shared dashboard for the organization.) • Can view event retention settings (View the settings for event retention.) • Can view shared searches (View the list of shared searches including the definition.) • Can run quick search searches (Run quick searches against all data.) • Can view event details (Allows the viewing of all event details.)
Audit Operator	• Can manage alerts (View, manage, create, and delete alerts, view the list of alert plans including their detailed configuration.) • Can export search results (Can export search results to a csv or csv.zip file.) • Can manage private searches (Create and modify private searches and manage search categories.) • Can run private searches (Run and preview searches.) • Can run search visualization (Run a search visualization.) • Can run shared searches (Run and preview shared searches.) • Can view dashboard (View the shared dashboard for the organization.) • Can view event retention settings (View the settings for event retention.) • Can view shared searches (View the list of shared searches including the definition.) • Can run quick search searches (Run quick searches against all data.) • Can view event details (Allows the viewing of all event details.)

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.

Customer data storage

On Demand Audit optionally allows one or more on premises installations of Change Auditor to be integrated into an On Demand Audit organization. An On Demand Audit organization must be selected for each connected Change Auditor installation. The selected On Demand organization determines the storage location of all customer data, and the On Demand Audit Azure region to which Change Auditor will transmit on premises Change Auditor event data. In the same manner as other data is handled, On Demand Audit ensures that on premises data remains within the same Azure data center regions outlined above.

Customers must select an organization in the correct region for their data residency requirements depending on their individual requirements and configuration for each installation of Change Auditor. All on premises data from Change Auditor is transmitted and retained in the selected On Demand organization and region. Depending on the configuration and global deployment of Change Auditor, customers can configure On Demand so that the On Demand organization will store data from multiple on premises global locations in a single On Demand organization region. In a similar manner, the customer could configure On Demand Audit to transmit data from on premises Change installations across a regional geographic boundary.

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 in US region, Change Auditor clients and coordinators must be able to access:

- https://quest-on-demand.com
- https://odauditprod-wus297293-api.azure-api.net

To create a configuration with On Demand Audit in Europe region, Change Auditor clients and coordinators must be able to access:

- https://quest-on-demand.com
- https://odauditprod-neur5293-api.azure-api.net

To create a configuration with On Demand Audit in the Canada region, Change Auditor clients and coordinators must be able to access:

- https://quest-on-demand.com
- https://odauditprod-ccan4293-api.azure-api.net

To create a configuration with On Demand Audit in the UK region, Change Auditor clients and coordinators must be able to access:

- https://quest-on-demand.com
- https://odauditprod-suk3293-api.azure-api.net

To create a configuration with On Demand Audit in the Australia region, Change Auditor clients and coordinators must be able to access:

- https://quest-on-demand.com
- https://odauditprod-eau6293-api.azure-api.net

To send events to On Demand Audit in US region, Change Auditor coordinators must be able to access:

- https://odauditprod-wus297293-iot.azure-devices.net

To send events to On Demand Audit in Europe region, Change Auditor coordinators must be able to access:

- https://odauditprod-neur5293-iot.azure-devices.net

To send events to On Demand Audit in the Canada region, Change Auditor coordinators must be able to access

- https://odauditprod-ccan4293-iot.azure-devices.net

To send events to On Demand Audit in the UK region, Change Auditor coordinators must be able to access

- https://odauditprod-suk3293-iot.azure-devices.net

To send events to On Demand Audit in the Australia region, Change Auditor coordinators must be able to access

- https://odauditprod-eau6293-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.

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.

NOTE: You can also export the search results to a .csv or zip file by selecting the Export button. The location for the file is determined by your browser settings.

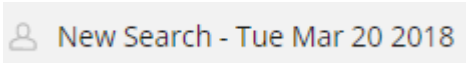
Working with searches

- 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.

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 Built in searches
- Azure Active Directory built in searches
- Best Practices built in searches
- Group Policy built in searches
- Logon Activity built in searches
- Office 365 built in searches
- Teams 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

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

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

Best Practices built in searches

On Demand Audit provides the following Best Practices built-in search:

- Sharing operations on important file types within past 7 days
- Teams guest access enabled or disabled in the past 30 days

Group Policy built in searches

On Demand Audit provides the following Group Policy built-in searches:

- Group Policy all events in the past 7 days
- Group Policy all restricted group changes in the past 30 days
- Group Policy all security changes in the past 30 days

Logon Activity built in searches

On Demand Audit provides the following logon activity built-in searches:

- Logon Activity all authentication activity in the past 7 days
- Logon Activity all excessive Kerberos ticket lifetime events in the past 30 days
- Logon Activity all failed logon activity in the past 7 days
- Logon Activity all interactive logon activity in the past 24 hours
- Logon Activity all Kerberos authentication activity in the past 24 hours
- Logon Activity all logon activity in the past 24 hours
- Logon Activity all logon session activity in the past 24 hours
- Logon Activity all NTLM version 1 logons in the past 7 days (Note: The associated event class is disabled by default in Change Auditor.)
- Logon Activity all remote logon activity in the past 24 hours

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

Teams built in searches

On Demand Audit provides the following Teams searches:

- Teams app events in the past 7 days
- Teams bot events in the past 7 days

- Teams channel events in the past 7 days
- Teams client configuration changes in the past 30 days
- Teams connector events in the past 7 days
- Teams events in the past 7 days
- Teams guest access configuration changes in the past 30 days
- Teams guest members added in the past 7 days
- Teams member role changes in the past 7 days
- Teams member changes in the past 7 days
- Teams notification and feeds policy changes in the past 30 days
- Teams organization setting changes in the past 30 days
- Teams tab events in the past 7 days
- Teams targeting policy changes in the past 30 days
- Teams team created events in the past 30 days
- Teams team deleted events in the past 30 days
- Teams team setting changes in the past 7 days
- Teams user sign-in events in the past 7 days

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.
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**.By default, the new search will be created in the category you have selected when clicking **New Search**. If required select a different category.
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.

Exporting a search

NOTE:

- 50 000 is the maximum number of results that can be exported at once. You will need to refine the search before exporting if the results exceed this number.
- The maximum download size is 250 MB. If this size is reached, only complete results will be included, the rest will be truncated. For searches with a large number of results, the ZIP option should be used.

To export a search

1. Select the **Searches** tab.
2. Locate the required search in the list of categories.
3. Run the search.
4. From the **Export** button, select to export to a CSV or CSV as ZIP file. The location for the file is determined by your browser settings.

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 .export the results to a .csv or .csv zip file. See Exporting a search for details.
- 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)

For Azure Active Directory, Active Directory, and Group Policy events, the summary also displays the following:

- Property After Value
- Property Before Value
- Property Name

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: A built-in private category.
- 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 events.

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 90 days

NOTE: Azure Active Directory Premium P2 subscription is required to include the Risk Level and Risk Detail information in events.

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

Audit module	Columns
	• 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 Membership Event	Target	Subject
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.

Auditing Office 365

On Demand Audit audits activity for Exchange Online, OneDrive for Business, Teams, and SharePoint Online 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.
- Teams user and administrator activity such as when teams (and associated settings, members, and applications) are created, updated, removed and when users sign in.

For details on running the searches and creating custom searches based off the built in searches, see:

- Using built in searches
- Office 365 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

Filter	Value to enter/ available pre-defined values to select
Action	Select from the following pre-defined values: • Add Attribute • Add Object • Delete Attribute • Delete Object • Modify Attribute • Move Object • Other Actions • Rename Object
Activity	• Enter an associated value
Activity Category	• AD Query • Anonymous Cloud Activity • Anonymous Web Site Activity • Authentication Activity • Authentication Services Monitoring • Azure Active Directory • Azure Active Directory - Administrative Units • Azure Active Directory - Application • Azure Active Directory - B2B

Filter	Value to enter/ available pre-defined values to select
	• Azure Active Directory - Directory • Azure Active Directory - Group • Aure Active Directory - Policy • Azure Active Directory - Resource • Azure Active Directory - Risk Event • Azure Active Directory - Role • Azure Active Directory - Sign-in • Azure Active Directory - User • Change Auditor Internal Auditing • Configuration Monitoring • Connection Object • Custom AD Object Monitoring • Custom ADAM Object Monitoring • Custom Computer Monitoring • Custom File System Monitoring • Custom Group Monitoring • Custom Registry Monitoring • Custom User Monitoring • Defender • DNS Service • DNS Zone • Domain Configuration • Domain Controller Authentication • Dynamic Access Control • EMC • Exchange ActiveSync Monitoring • Exchange Administrative Group • Exchange Distribution List • Exchange Mailbox Monitoring • Exchange Organization

Filter	Value to enter/ available pre-defined values to select
	• Exchange Permission Tracking • Exchange Security Group • Exchange User • Fault Tolerance • File System Access Denied • File System Configuration Change • File System Content Change • File System Content Access • File System Security Change • FluidFS • Forest Configuration • FRS Service • Group Policy Item • Group Policy Object • Group Monitoring • IP Security • Local Group Monitoring • Local User Monitoring • Logon Session • NetApp • NETLOGON Service • None • NTDS Service • Office 365 Exchange Online Administration • Office 365 SharePoint Online • Office 365 OneDrive for Business • Office 365 Exchange Online Mailbox • OU • Replication Transport • Schema Configuration • Security Change Detail

Filter	Value to enter/ available pre-defined values to select
	• Service Monitoring • SharePoint Document • SharePoint Document Library • SharePoint Farm • SharePoint Folder • SharePoint List • SharePoint List Item • SharePoint Permission • SharePoint Security Group • SharePoint Site • SharePoint Site Collection • Site Configuration • Site Link Bridge Configuration • Site Link Configuration • Skype for Business Administration • Skype for Business Configuration • SQL Broker Event • SQL CLR Event • SQL Cursors Event • SQL Data Level • SQL Database Event • SQL Deprecation Event • SQL Errors and Warnings Event • SQL Full Text Event • SQL Locks Event • SQL Objects Event • SQL OLEDB Event • SQL Performance Event • SQL Progress Report Event • SQL Query Notifications Event

Filter	Value to enter/ available pre-defined values to select
	• SQL Scan Event • SQL Security Audit Event • SQL Server Event • SQL Session Event • SQL Stored Procedures Event • SQL Transaction Event • SQL TSQL Event • SQL User-Configurable Event • Subnets • System Events • SYSVOL • Threat Detection - Alert • Threat Detection - Risky User • User Cloud Activity • User Web Site Activity • VMware Account • VMware Alarm • VMware Authorization • VMware Cluster • VMware Custom Field • VMware Datacenter • VMware Datastore • VMware DVPortgroup • VMware Dvs • VMware Generic • VMware Host • VMware License • VMware Profile • VMware Resource Pool

Filter	Value to enter/ available pre-defined values to select
	• VMware Scheduled Task • VMware Session • VMware Task • VMware Template Upgrade • VMware Upgrade • VMware Virtual Machine
Activity Id	• Enter an associated value
Activity Time	• Enter days or hours
Actor Id	• Enter an associated value
Actor Name	• Enter an associated value
Actor Object Id	• Enter an associated value
Actor PUID	• Enter an associated value
Actor Service Principle Name	• Enter an associated value
Actor User Principal Name	• Enter an associated value
AD Authorization Port	• Enter an associated value
AD Kerberos	• Enter an associated value
AD Security Change Applies To	• Enter an associated value
AD Security Change Condition	• Enter an associated value
AD Security Change Permission	• Enter an associated value
AD Security Change Type	• Enter an associated value
AD Simple Bind	• Enter an associated value
AD SSL/TLS	• Enter an associated value
Additional Details	• Enter an associated value
Additional Info	• Enter an associated value
Add-on Guid	• Enter an associated value
Add-on Name	• Enter an associated value
Add-on Type	Select from the following pre-defined values: • Bot • Connector • Tab

Filter	Value to enter/ available pre-defined values to select
	• App
Affected Items	• Enter an associated value
Agent Domain Fully Qualified Domain Name	• Enter an associated value
Agent Forest Name	• Enter an associated value
Agent Fully Qualified Domain Name	• Enter an associated value
Agent Id	• Enter an associated value
Agent OS Version	• Enter an associated value
Agent Site Name	• Enter an associated value
Alert Recipients	• Enter an associated value
Application Id	• Enter an associated value
Application Name	• Enter an associated value
Attribute Name	• Enter an associated value
Atypical Location	Select from the following pre-defined values: • Yes • No
Audit Item	• Enter an associated value
Audit Source	• Enter an associated value
Authentication Protocol	Select from the following pre-defined values: • Kerberos • NTLM • Unknown
Authentication Protocol Version	Select from the following pre-defined values: • V1 • V2
Azure AD Activity Operation Type	• Enter an associated value
Azure AD Activity Type	• Enter an associated value
Azure AD Category	• Enter an associated value
Azure AD Result Description	• kEnter an associated value
Channel Name	• Enter an associated value
Channel Guid	• Enter an associated value

Filter	Value to enter/ available pre-defined values to select
Channel Type	Select from the following pre-defined values: • Private • Standard
Change Auditor Event Class ID	• Enter an associated value
Change Auditor Event Class Name	• Enter an associated value
Change Auditor Facility ID	• Enter an associated value
Change Auditor Facility Name	• Enter an associated value
City	• Enter an associated value
Client Info String	• Enter an associated value
Client IP Address	• Enter an associated value
Client Machine Name	• Enter an associated value
Client Process Name	• Enter an associated value
Client Version	• Enter an associated value
Cmdlet Name	• Enter an associated value
Comment	• Enter an associated value
Coordinator Id	• Enter an associated value
Correlation Id	• Enter an associated value
Country	• Enter an associated value
Cross-Mailbox Operations	• Enter an associated value
Custom Event	• Enter an associated value
Destination File Extension	• Enter an associated value
Destination FileName	• Enter an associated value
Destination Folder	• Enter an associated value
Destination MailboxId Id	• Enter an associated value
Destination MailboxId Owner Master Account Sid	• Enter an associated value
Destination MailboxId Owner Sid	• Enter an associated value
Destination MailboxId Owner UPN	• Enter an associated value
Destination relative URL	• Enter an associated value
Detection Timing	Select from the following pre-defined values:

Filter	Value to enter/ available pre-defined values to select
	• Near Realtime • Not Defined • Offline • Realtime
Device Information	• Enter an associated value
Distribution Group Name	• Enter an associated value
Domain Name	• Enter an associated value
Error Code	• Enter an associated value
Event Data	• Enter an associated value
Event Id	• Enter an associated value
Event Source	• Enter an associated value
Event Source Application	• Enter an associated value
Event Version	• Enter an associated value
External Access	• Enter an associated value
Failure Reason	• Enter an associated value
Folder	• Enter an associated value
Initiator User Mail	• Enter an associated value
Initiator User Name	• Enter an associated value
Initiator User SID	• Enter an associated value
Installation Id	• Enter an associated value
Internal Correlation Id	• Enter an associated value
Is Linked Group Policy Change	Select from the following pre-defined values: • False • True
Item type	• Enter an associated value
Kerberos Ticket Lifetime (Hours)	• Enter an associated value
Logon Begin Type	Select from the following pre-defined values: • Additional logon • Concurrent user disconnected • Existing logon

Filter	Value to enter/ available pre-defined values to select
	• Lock • Logoff • Logon • None • Remote logoff • Remote logon • Screensaver turned off • Screensaver turned on • Shutdown • Unlock
Logon Duration	• Enter an associated value
Logon End	• Enter days or hours
Logon End Type	Select from the following pre-defined values: • Additional logon • Concurrent user disconnected • Existing logon • Lock • Logoff • Logon • None • Remote logoff • Remote logon • Screensaver turned off • Screensaver turned on • Shutdown • Unlock
Logon Session End	• Enter days or hours
Logon Session Start	• Enter days or hours
Logon Start	• Enter days or hours
Logon Type (Exchange Online)	Select from the following pre-defined values: • Admin • Best Access

Filter	Value to enter/ available pre-defined values to select
	• Delegated • Delegated Admin • Owner • System Service • Transport • Unknown
Logon Type (Windows)	Select from the following pre-defined values: • None • Remote Interactive • Domain Authentication • User Session • Interactive • Network • All
Logon User Display Name	• Enter an associated value
Logon User Sid	• Enter an associated value
Machine Domain Info	• Enter an associated value
Machine Id	• Enter an associated value
Mailbox Guid	• Enter an associated value
Mailbox Name	• Enter an associated value
Mailbox Owner Master Account Sid	• Enter an associated value
Mailbox Owner Sid	• Enter an associated value
Mailbox Owner UPN	• Enter an associated value
Malware Name	• Enter an associated value
MFA Authentication Detail	• Enter an associated value
MFA Authentication Method	• Enter an associated value
MFA Required	Select from the following pre-defined values: • Yes • No
MFA Result	• Enter an associated value
Modified Object	• Enter an associated value

Filter	Value to enter/ available pre-defined values to select
Modified Properties	• Enter an associated value
NTLM Impersonation Level	Select from the following pre-defined values: • Default • Anonymous • Identify • Impersonate • Delegate
NTLM Key Length	• Enter an associated value
Object Id	• Enter an associated value
Office365 Organization Id	• Enter an associated value
Organization Name	• Enter an associated value
Origin AD Site Name	• Enter an associated value
Origin IP Address	• Enter an associated value
Origin IPv4 Address	• Enter an associated value
Origin IPv6 Address	• Enter an associated value
Origin Name	• Enter an associated value
Originating Server	• Enter an associated value
Parameters	• Enter an associated value
Parent Event Id	• Enter an associated value
Policy Setting	• Access Credential Manager as a trusted caller • Access This Computer From The Network • Account Lockout Duration • Account Lockout Threshold • Account Logon: Audit Credential Validation • Account Logon: Audit Kerberos Authentication Service • Account Logon: Audit Kerberos Service Ticket Operations • Account Logon: Audit Other Account Logon Events • Account Management: Audit Application Group Management

Filter	Value to enter/ available pre-defined values to select
	• Account Management: Audit Computer Account Management • Account Management: Audit Distribution Group Management • Account Management: Audit Other Account Management Events • Account Management: Audit Security Group Management • Account Management: Audit User Account Management • Accounts: Administrator Account Status • Accounts: Guest Account Status • Accounts: Limit Local Account Use Of Blank Passwords To Console Logon Only • Accounts: Rename Administrator Account • Accounts: Rename Guest Account • Act As Part Of The Operating System • Add Workstations To Domain • Adjust Memory Quotas For A Process • Allow Log On Locally • Allow Log On Through Terminal Services • Application Data Folder options • Application Data Folder target path • Audit Account Logon Events • Audit Account Management • Audit Directory Service Access • Audit Logon Events • Audit Object Access • Audit Policy Change • Audit Privilege Use • Audit Process Tracking

Filter	Value to enter/ available pre-defined values to select
	• Audit System Events • Audit: Audit The Access Of Global System Objects • Audit: Audit The Use Of Backup And Restore Privilege • Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings • Audit: Shut Down System Immediately If Unable To Log Security Audits • Authenticode Settings Enable Trusted Publisher Lockdown option • Autoenrollment Settings • Automatic Browser Configuration Auto-config URL • Automatic Browser Configuration Automatic Configuration option • Automatic Browser Configuration Automatic Configuration Time • Automatic Browser Configuration Automatic detection option • Automatic Browser Configuration Auto-proxy URL • Automatic Certificate Request Settings • Back Up Files And Directories • Basic User Hash Rule • Basic User Zone Rule • BitLocker Drive Encryption • Browser Title • Bypass Traverse Checking • Central Access Policy • Change The System Time • Change the time zone • Computer Configuration Administrative Template • Computer Preference Setting

Filter	Value to enter/ available pre-defined values to select
	• Connection Settings Delete Existing Option • Connection Settings Import Option • Contacts Folder target path • Content Ratings option • Create A Pagefile • Create A Token Object • Create Global Objects • Create Permanent Shared Objects • Create symbolic links • Custom Large Static Logo • Custom Small Animated Logo • Custom Small Static Logo • Debug Programs • Default Security Level • Delete Existing Channels option • Delete Existing Favorites option • Deny Access To This Computer From The Network • Deny Log On As A Batch Job • Deny Log On As A Service • Deny Log On Locally • Deny Log On Through Terminal Services / Remote Desktop Services • Designated File Types • Desktop Folder options • Desktop Folder target path • Detailed Tracking: Audit DPAPI Activity • Detailed Tracking: Audit Process Creation • Detailed Tracking: Audit Process Termination • Detailed Tracking: Audit RPC Events

Filter	Value to enter/ available pre-defined values to select
	• Devices: Allow Undock Without Having To Logon • Devices: Allowed To Format And Eject Removable Media • Devices: Prevent Users From Installing Printer Drivers • Devices: Restrict CD-ROM Access To Locally Logged-On User Only • Devices: Restrict Floppy Access To Locally Logged-On User Only • Devices: Unsigned Driver Installation Behavior • Disallowed Certificate Rule • Disallowed Hash Rule • Disallowed Path Rule • Disallowed Zone Rule • Domain Controller: Allow Server Operators To Schedule • Domain Controller: LDAP Server Signing Requirements • Domain Controller: Refuse Machine Account Password C • Domain Member: Digitally Encrypt Or Sign Secure Channel Data (Always) • Domain Member: Digitally Encrypt Secure Channel Data (When Possible) • Domain Member: Digitally Sign Secure Channel Data (When Possible) • Domain Member: Disable Machine Account Password Changes • Domain Member: Maximum Machine Account Password Age • Domain Member: Require Strong (Windows 2000 Or Later) Session Key • Downloads Folder options • Downloads Folder target path

Filter	Value to enter/ available pre-defined values to select
	• DS Access: Audit Detailed Directory Service Replication • DS Access: Audit Directory Service Access • DS Access: Audit Directory Service Changes • DS Access: Audit Directory Service Replication • Enable Computer And User Accounts To Be Trusted For Delegation • Encrypting File System • Enforce Password History • Enforce User Logon Restrictions • Enforcement Files • "Enforcement Users • Enterprise Trust • "Favorites List • Favorites options • Favorites target path • File or Folder • Force Shutdown From A Remote System • Generate Security Audits • Global Object Access Auditing: File system • Global Object Access Auditing: Registry • Group Policy Container Access • Group policy disable computer configuration flag • Group policy disable user configuration flag • Group policy WMI Filter • Impersonate A Client After Authentication • Important URLs Home Page URL • Important URLs Online Support URL • Important URLs Search Bar URL • Increase a process working set

Filter	Value to enter/ available pre-defined values to select
	• Increase Scheduling Priority • Interactive Logon: Display user information when the session is locked • Interactive Logon: Do Not Display Last User Name • Interactive Logon: Do Not Require CTRL+ALT+DEL • Interactive Logon: Message Text For Users Attempting To Log On • Interactive Logon: Message Title For Users Attempting To Log On • Interactive Logon: Number Of Previous Logons To Cache (In Case Domain Controller Is Not Available) • Interactive Logon: Prompt User To Change Password Before Expiration • Interactive Logon: Require Domain Controller Authentication To Unlock Workstation • Interactive Logon: Require Smart Card • Interactive Logon: Smart Card Removal Behavior • Intermediate Certificate Authorities • IP Security Policy • Links Folder options • Links Folder target path • Links List • Load And Unload Device Drivers • Lock Pages In Memory • Log On As A Batch Job • Log On As A Service • Logon/Logoff: Audit Account Lockout • Logon/Logoff: Audit IPsec Extended Mode • Logon/Logoff: Audit Logon • Logon/Logoff: Audit Network Policy Server • Logon/Logoff: Audit Other Logon/Logoff Events

Filter	Value to enter/ available pre-defined values to select
	• Logon/Logoff: Audit Special Logon • Machine Access Restrictions in Security Descriptor Definition Language (SDDL) syntax • Machine Launch Restrictions in Security Descriptor Definition Language (SDDL) syntax • Manage Auditing And Security Log • Maximum Application Log Size • Maximum Lifetime For Service Ticket • Maximum Lifetime for User Ticket • Maximum Lifetime For User Ticket Renewal • Maximum Password Age • Maximum Security Log Size • Maximum System Log Size • Maximum Tolerance for Computer Clock Synchronization • Microsoft Network Client: Digitally Sign Communications (Always) • Microsoft Network Client: Digitally Sign Communications (If Server Agrees) • Microsoft Network Client: Send Unencrypted Password To Connect To Third-Party SMB Servers • Microsoft Network Server: Amount Of Idle Time Required Before Suspending Session • Microsoft Network Server: Digitally Sign Communication (Always) • Microsoft Network Server: Digitally Sign Communications (If Client Agrees) • Microsoft Network Server: Disconnect Clients When Logon Hours Expire • Microsoft network server: Server SPN target name validation level • Minimum Password Age • Minimum Password Length

Filter	Value to enter/ available pre-defined values to select
	• Modify Firmware Environment • Music Folder options • Music Folder target path • My Documents Folder options • My Documents Folder Redirection: My Pictures Options • My Documents Folder target path • NAP Client Health Registration Settings: CSP • NAP Client Health Registration Settings: CSP Key Length • NAP Client Health Registration Settings: Hash Algorithm • NAP Client Health Registration Settings: Require server verification • NAP Client Health Registration Settings: Trusted server group • NAP Client Health Registration Settings: Trusted server URL • NAP Enforcement Clients: DHCP Quarentine Enforcement Client • NAP Enforcement Clients: IPsec Relying Party • AP Enforcement Clients: RD Gateway Quarentine Enforcement Client • NAP Enforcement Clients: Remote access enforcement client for Windows XP and Windows Vista • NAP Enforcement Clients: Wireless EAPOL enforcement client for Windows XP • NAP User Interface Settings: Description changed • NAP User Interface Settings: Image File changed • NAP User Interface Settings: Image File Name changed • NAP User Interface Settings: Title changed

Filter	Value to enter/ available pre-defined values to select
	• Network Access: Allow Anonymous SID/Name Translation • Network Access: Do Not Allow Anonymous Enumeration Of SAM Accounts • Network Access: Do Not Allow Anonymous Enumeration Of SAM Accounts And Shares • Network Access: Do Not Allow Storage Of Credentials Or .NET Passports For Network Authentication • Network Access: Let Everyone Permissions Apply To Anonymous Users • Network Access: Named Pipes That Can Be Accesssed Anonymously • Network Access: Remotely Accessible Registry Paths • Network Access: Remotely Accessible Registry Paths And Sub-Paths • Network Access: Restrict Anonymous Access To Named Pipes and Shares • Network Access: Shares That Can Be Accessed Anonymously • Network Access: Sharing And Security Model For Local Accounts • Network Security: Allow Local System to use computer identity for NTLM • Network security: Allow LocalSystem NULL session fallback • Network security: Allow PKU2U authentication requests to this computer to use online identities • Network security: Configure encryption types allowed for Kerberos • Network Security: Do Not Store LAN Manager Hash Value On Next Password Change • Network Security: Force Logoff When Logon Hours Expire • Network Security: LAN Manager Authentication Level

Filter	Value to enter/ available pre-defined values to select
	• Network Security: LDAP Client Signing Requirements • Network Security: Minimum Session Security For NTLM SSP Based (Including Secure RPC) Clients • Network Security: Minimum Session Security For NTLM SSP Based (Including Secure RPC) Servers • Network security: Restrict NTLM: NTLM authentication in this domain • Network security: Restrict NTLM: Add remote server exceptions for NTLM authentication • Network security: Restrict NTLM: Add server exceptions in this domain • Network security: Restrict NTLM: Audit Incoming NTLM Traffic • Network security: Restrict NTLM: Audit NTLM authentication in this domain • Network security: Restrict NTLM: Incoming NTLM traffic • Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers • NLM: Location type • NLM: Location type permissions • NLM: Network icon permissions • NLM: Network name • NLM: Network name permissions • Object Access: Audit Application Generated • Object Access: Audit Certification Services • Object Access: Audit File Share • Object Access: Audit File System • Object Access: Audit Filtering Platform Connection • Object Access: Audit Filtering Platform Packet Drop • Object Access: Audit Handle Manipulation • Object Access: Audit Kernel Object

Filter	Value to enter/ available pre-defined values to select
	• Object Access: Audit Other Object Access Events • Object Access: Audit Registry • Object Access: Audit SAM • Object Access: Detailed File Share • Password Must Meet Complexity Requirements • Perform Volume Maintenance Tasks • Pictures Folder options • Pictures Folder target path • Place Favorites At Top Of List option • Policy Change: Audit Authentication Policy Change • Policy Change: Audit Authorization Policy Change • Policy Change: Audit Filtering Platform Policy Change • Policy Change: Audit MPSSVC Rule-Level Policy Change • Policy Change: Audit Other Policy Change Events • Policy Change: Audit Policy Change • Prevent Local Guests Group From Accessing Application Log • Prevent Local Guests Group From Accessing Security Log • Prevent Local Guests Group From Accessing System Log • Privilege Use: Audit Non Sensitive Privilege Use • Privilege Use: Audit Other Privilege Use Events • Privilege Use: Audit Sensitive Privilege Use • Profile System Performance • Program Settings option • Proxy Settings Exceptions • Proxy Settings FTP Proxy • Proxy Settings Gopher Proxy

Filter	Value to enter/ available pre-defined values to select
	• Proxy Settings HTTP Proxy • Proxy Settings Secure Proxy • Proxy Settings Socks Proxy • QoS Policy: Application Name • QoS Policy: DSCP Value • QoS Policy: Local IP • QoS Policy: Local IP Prefix Length • QoS Policy: Local Port • QoS Policy: Protocol • QoS Policy: Remote IP • QoS Policy: Remote IP Prefix Length • QoS Policy: Remote Port • QoS Policy: Throttle Rate • QoS Policy: URL • QoS Policy: URL Recursive • QoS Policy: Version • Recovery Console: Allow Automatic Administrative Logon • Recovery Console: Allow Floppy Copy And Access To All Drives And All Folders • Registry key • Remove Computer From Docking Station • Replace A Process Level Token • Reset Account Lockout Counter After Change • Restore Files And Directories • Restricted Group • Restricted Group Member • Restricted Group Membership • Retain Application Log • Retain Security Log

Filter	Value to enter/ available pre-defined values to select
	• Retain System Log • Retention Method For Application Log • Retention Method For Security Log • Retention Method For System Log • Saved Games Folder target path • Script setting • Searches Folder options • Searches Folder target path • Secure System Partition (For RISC Platforms Only) • Security Zones and Privacy option • Shut Down The Computer When The Security Audit Log Is Full • Shut Down The System • Shutdown: Allow System To Be Shut Down Without Having To Log On • Shutdown: Clear Virtual Memory Pagefile • Software Installation Policy • Start Menu Folder options • Start Menu Folder target path • Starter GPO • Starter GPO Computer setting • Starter GPO User setting • Store Passwords Using Reversible Encryption • Synchronize Directory Service Data • System Cryptography: Force Strong Key Protection For User Keys Stored On The Computer policy • System Cryptography: Use FIPS Compliant Algorithms For Encryption, Hashing, and Signing policy • System Objects: Default Owner For Objects Created By Members Of The Administrators Group policy

Filter	Value to enter/ available pre-defined values to select
	• System Objects: Require Case Insensitivity For Non-Windows Subsystems policy • System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links) policy • System Services Policy Service • System Services Policy Service Startup Mode • System Settings: Optional Subsystems • System Settings: Use Certificate Rules On Windows Executables For Software Restriction Policies • System: Audit IPsec Driver • System: Audit Other System Events • System: Audit Security State Change • System: Audit Security System Extension • System: Audit System Integrity • Take Ownership Of Files Or Other Objects • Toolbar background Bitmap • Toolbar Buttons • Trusted People • Trusted Publishers • Trusted Root Certification Authority • Unrestricted Certificate Rule • Unrestricted Hash Rule • Unrestricted Path Rule • Unrestricted Zone Rule • Unsigned Non-Driver Installation Behavior • User Account Control: Admin Approval Mode for the Built-in Administrator account • User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop • User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode

Filter	Value to enter/ available pre-defined values to select
	• User Account Control: Behavior of the elevation prompt for standard users • User Account Control: Detect application installations and prompt for elevation • User Account Control: Only elevate executables that are signed and validated • User Account Control: Only elevate UIAccess applications that are installed in secure locations • User Account Control: Run all administrators in Admin Approval Mode • User Account Control: Switch to the secure desktop when prompting for elevation • User Account Control: Virtualize file and registry write failures to per-user locations • User Administrative Template setting • User Agent String • User Credential Roaming • User Credential Roaming Options • User Group Policy Preference • User Software Restriction Basic User Hash Rule • User Software Restriction Basic User Path Rule • User Software Restriction Basic User Zone Rule • User Software Restriction Designated File Types • User Software Restriction Disallowed Certificate Rule • User Software Restriction Disallowed Hash Rule • User Software Restriction Disallowed Path Rule • User Software Restriction Disallowed Zone Rule • User Software Restriction Enforcement Files • User Software Restriction Enforcement Users • User Software Restriction Policies Default Security Level

Filter	Value to enter/ available pre-defined values to select
	• User Software Restriction Trusted Publishers • User Software Restriction Unrestricted Certificate Rule • User Software Restriction Unrestricted Hash Rule • User Software Restriction Unrestricted Path Rule • User Software Restriction Unrestricted Zone Rule • Videos Folder options • Videos target path • Wireless Network Policy
Policy Setting Category	• Account Lockout Policy • Additional Rules • Administrative Templates: Policy definitions • Audit Policies • Audit Policy • Central Access Policy • Change Auditor Protection • Event Log • File System • Folder Redirection • GPO Status • Internet Explorer Maintenance • IP Security Policies on Active Directory • Kerberos Policy • NAP Client Configuration • Network List Manager Policies • Password Policy • Policy-Based QoS • Preferences • Public Key Policies

Filter	Value to enter/ available pre-defined values to select
	• Registry • Restricted Groups • Scripts (Logon/Logoff) • Scripts (Startup/Shutdown) • Security Levels • Security Options • Software Installation • Software Restriction Policies • Software Settings • Starter GPO • System Services • User Rights Assignment • Wireless Network Policies • WMI Filtering
Policy Setting List Item	• Enter an associated value
Policy Setting Location	• Enter an associated value
Previous City	• Enter an associated value
Previous Country	• Enter an associated value
Previous IP	• Enter an associated value
Previous Sign-in Time	• Enter days or hours
Previous State	• Enter an associated value
Previous User Agent	• Enter an associated value
Property Name	• Enter an associated value
Property Before Value	• Enter an associated value
Property After Value	• Enter an associated value
Record Type	• Enter an associated value
Request Id	• Enter an associated value
Result Status	• Enter an associated value
Risk Activity	Select from the following pre-defined values:

Filter	Value to enter/ available pre-defined values to select
	• Signin • User
Risk Correlation Id	• Enter an associated value
Risk Detail	Select from the following pre-defined values: • None • Admin Generated Temporary Password • User Performed Secured Password Change • User Performed Secured Password Reset • Admin Confirmed Signin Safe • Hidden • Admin Confirmed Signin Compromised • Admin Confirmed User Compromised • Admin Dismissed All Risk For User • Ai Confirmed Signin Safe • User Passed MFA Driven By Risk Based Policy
Risk Detected Time	• Enter days or hours
Risk Event Details	• Enter an associated value
Risk Event Id	• Enter an associated value
Risk Event Status	Select from the following pre-defined values: • Active • Closed (MFA Auto-Closed) • Closed (Multiple Reasons) • Closed (marked as false positive) • Closed (resolved) • Closed (ignored) • Login Blocked • Remediated
Risk Event Time	• Enter days or hours
Risk Event Type	Select from the following pre-defined values: • Anonymous IP Risk Event • Impossible Travel Risk Event • Leaked Credentials Risk Event

Filter	Value to enter/ available pre-defined values to select
	• Malware Risk Event • Suspicious IP Risk Event • Unfamiliar Location Risk Event
Risk Level	Select from the following pre-defined values: • Hidden • High • Low • Medium • None
Risk Source	• Enter an associated value
Risk State	Select from the following pre-defined values: • At Risk • Confirmed Compromised • Confirmed Safe • Dismissed • None • Remediated
Risk Type	Select from the following pre-defined values: • Unlikely Travel • Anonymized IP Address • Malicious IP Address • Unfamiliar Features • Malware Infected IP Address • Suspicious IP Address • Leaked Credentials • Investigations Threat Intelligence • Generic Admin Confirmed User Compromised • Mcas Impossible Travel • Mcas Suspicious Inbox Manipulation Rules • Investigations Threat Intelligence Signin Linked • Malicious IP Address Valid Credentials Blocked IP
Schema Id	• Enter an associated value

Filter	Value to enter/ available pre-defined values to select
Send as User Mailbox Guid	• Enter an associated value
Send as User SMTP	• Enter an associated value
Send on behalf of User Mailbox Guid	• Enter an associated value
Send on behalf of User SMTP	• Enter an associated value
Service	Select from the following pre-defined values: • Active Directory • Azure Active Directory • Exchange • Group Policy • Logon Activity • On Demand Audit • OneDrive • SharePoint • Teams
Severity	Select from the following pre-defined values: • High • Low • Medium
Sharing Target	• Enter an associated value
Sharing Target Type	• Enter an associated value
Sharing Type	• Enter an associated value
Site	• Enter an associated value
Siter Url	• Enter an associated value
Source File Extesion	• Enter an associated value
Source File Name	• Enter an associated value
Source Folders	• Enter an associated value
Source Name	• Enter an associated value
Source relative Url	• Enter an associated value
State	• Enter an associated value
Status	Select from the following pre-defined values: • Failed

Filter	Value to enter/ available pre-defined values to select
	• Successful
Status Reason (Change Auditor)	Selectfrom the following pre-defined values: • Failed • Protected • Succeeded
Subject	• Enter an associated value
Subject Name	• Enter an associated value
Subject Object Id	• Enter an associated value
Subject PUID	• Enter an associated value
Subject Resource Type	• Enter an associated value
Subject Service Principle Name	• Enter an associated value
Subject Type	• Enter an associated value
Subject User Principle Name	• Enter an associated value
Target	• Enter an associated value
Target AD Forest Name	• Enter an associated value
Target Additional Details	• Enter an associated value
Target Canonical Name	• Enter an associated value
Target Computer Name	• Enter an associated value
Target Distinguished Name	• Enter an associated value
Target Domain Name	• Enter an associated value
Target IP Address	• Enter an associated value
Target is Domain Controller	• Enter an associated value
Target Managed By	• Enter an associated value
Target Name	• Enter an associated value
Target Object Class	• Enter an associated value
Target Object Id	• Enter an associated value
Target Organizational Unit CN	• Enter an associated value
Target Parent Object Id	• Enter an associated value
Target Policy Item	• Enter an associated value
Target Policy Section	• Enter an associated value

Filter	Value to enter/ available pre-defined values to select
Target PUID	• Enter an associated value
Target Resource Type	• Enter an associated value
Target SAM Account Name	• Enter an associated value
Target Service Principle Name	• Enter an associated value
Target Site Name	• Enter an associated value
Target Type	• Enter an associated value
Target User Mail	• Enter an associated value
Target User Principle Name	• Enter an associated value
Team Guid	• Enter an associated value
Team Name	• Enter an associated value
Teams Property Name	Select from the following pre-defined values: • Allow Box in Files tab • Accepted channel SMTP domains list • Allow DropBox in Files tab • Allow Egnyte in Files tab • Allow Guest access in Teams • Allow Google Drive in Files tab • Allow Resource Account Send Messages • Allow Share File in Files tab • Allow Skype for Business Interop • Allow TBot Proactive Messaging • Allow users to send emails to channels • Guests allow IP video • Guests screen sharing mode • Guests allow Meet Now • Guests allow editing of sent messages • Guests allow Deletion of sent messages • Guests allow chat • Guests allow Giphys in conversations

Filter	Value to enter/ available pre-defined values to select
	• Guests Giphy content rating • Guests allow memes in conversations • Guests use Stickers in conversations • Guests allow immersive reader • Guests allow private calls • Meeting room device content pin • Members can add additional tags • Resource Account Content Access • Show organization tab in chats • Suggested default tags • Suggested feeds appear in user's activity feed • Trending feeds appear in user's activity feed • Tagging permission mode • Team owners can override who can apply tags • Use Exchange address book policy
Teams Role Type	Select from the following pre-defined values: • Member • Owner • Guest
Tenant Id	• Enter an associated value
Tenant Name	• Enter an associated value
Time Detected	• Enter days or hours
Time Indexed	• Enter days or hours
Time Received	• Enter days or hours
Token Issuer	Select from the following pre-defined values: • AD Federation Services • Azure AD
Url	• Enter an associated value
User (Actor)	• Enter an associated value

Filter	Value to enter/ available pre-defined values to select
User Agent	• Enter an associated value
User Display Name	• Enter an associated value
User DN	• Enter an associated value
User Down-level Logon Name	• Enter an associated value
User Id	• Enter an associated value
User is Administrator	Select from the following pre-defined values: • False • True • Unknown
User Key	• Enter an associated value
User Mail	• Enter an associated value
User Organizational Unit	• Enter an associated value
User Session Detail	Select from the following pre-defined values: • Computer lock/unlock • Computer restart/shutdown • Incorrectly finished • Screensaver • Started before session monitoring service • Terminal services connection • User logon/logoff • User switch
User Shared With	• Enter an associated value
User SID	• Enter an associated value
User Type	• Enter an associated value

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.

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