Quest

Quest On Demand Audit

User Guide

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

June, 24 2024

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
- 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 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 Microsoft 365 Security & Compliance Center unified audit log. See Auditing Microsoft 365 for details.
- Azure Active Directory user, group, application, and directory activity that corresponds to the events in the audit logs, sign-in activity report, and risky sign-ins report. See Auditing Azure Active Directory for details.

Accessing Quest On Demand Audit

On Demand management is based on the concepts of organizations. When you sign up for the On Demand service, you create an organization and you become the organization administrator. The organization can then subscribe to modules.

To access On Demand

1. Go to quest-on-demand.com
2. On the Welcome to Quest On Demand page, click **Sign in with Microsoft**.
3. Sign in using your Microsoft MFA-enabled account.
4. As part of the login process with Microsoft Entra ID, users must consent to the set of minimal permissions. By default, all users are allowed to consent to applications for permissions that do not require administrator consent. This behavior might be disabled in some Azure Active Directory tenants and may require tenant administrators to enable user consent flow for the Quest On Demand application.

For more 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
- United Kingdom
- United States

4

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:

- For details on adding your first tenant, refer to the On Demand Global Settings User Guide.
- GCC tenants are only supported by Audit in On Demand organizations located the US region.
- 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. To add another tenant, navigate to the **Audit** module. From the **Configuration** tab, click **Add Azure AD 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**.

   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 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 may need to turn on Office 365 audit logging. For more information, see Microsoft documentation.

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 **Audit** module.
2. Open the **Configuration** tab.
3. Select the services to audit for your tenant.
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 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	For services that were not enabled with a trial license, historical events are

Service	Changing from a trial license to a paid subscription
• Audit Logs • Sign-ins (and risk events)	collected for either 7 or 30 past days, depending on the Azure Active Directory report retention policies.
Change Auditor • Active Directory • Group Policy • Logon Activity • File System Activity	For services that were not enabled with a trial license, historical events are collected up to 30 days prior to upgrade to Change Auditor 7.0.0 (or higher).

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 **Settings**, expand **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
On Demand Administrator (Audit)	• Can Manage Azure Active Directory 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 Organization Private Alerts and Private Alert Plans (Can view and control all private alerts and private alert plans organization-wide.) • Can manage private alerts and alert plans (Can view and define their own private alerts and alert plans.) Can manage shared alerts and shared alert plans (Can view and define their own shared alerts and alert plans.) • Can manage private searches (Create and modify private searches and manage search categories.) • Can manage shared alerts and shared alert plans (Can view and define their own shared alerts and alert plans.) • Can manage shared searches (Can create and modify shared searches.) • Can run private searches (Run and preview searches.) • Can run quick search searches (Run quick searches against all data.) • Can run shared searches (Run and preview shared searches.) • Can view dashboard (View the shared dashboard for the organization.) • Can view event details (Allows the viewing of all event details.) • Can view event retention settings (View the settings for event retention.) • Can view shared searches (View the list of shared searches including the definition.)
Audit Administrator	• Can Manage Azure Active Directory 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 alerts and alert plans (Can view and define their own private alerts and alert plans.) • Can manage private searches (Create and modify private searches and manage search categories.) • Can manage shared alerts and shared alert plans (Can view and define their own shared alerts and alert plans.)

Role	Permission Details
	• Can manage shared searches (Can create and modify shared searches.) • Can export search results (Can export search results to a csv or csv.zip file.) • Can run private searches (Run and preview searches.) • Can run shared searches (Run and preview shared searches.) • Can run quick search searches (Run quick searches against all data.) • 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 view event details (Allows the viewing of all event details.)
Audit Operator	• Can manage private alerts and alert plans (Can view and define their own private alerts and alert plans.) • 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 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://id.quest.com
- https://us.core.api.quest-on-demand.com

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://id.quest.com
- https://eu.core.api.quest-on-demand.com

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://id.quest.com
- https://canada.core.api.quest-on-demand.com

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://id.quest.com
- https://uk.core.api.quest-on-demand.com

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://id.quest.com
- https://au.core.api.quest-on-demand.com

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
- https://odaudit97293data.blob.core.windows.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
- https://odaudit5293data.blob.core.windows.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
- https://odaudit4293data.blob.core.windows.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
- https://odaudit3293data.blob.core.windows.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
- https://odaudit6293data.blob.core.windows.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 **Audi** 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.

SpecterOps BloodHound Enterprise Integration

Attack path management is a critical component of defending Active Directory and Microsoft 365 environments from attacks. SpecterOps BloodHound Enterprise simplifies this process by prioritizing and quantifying attack path choke points, giving you the information you need to identify and eliminate the paths with the most exposure and risk.

Integrating with SpecterOps BloodHound Enterprise helps you reduce the risk of attacks by enabling you to easily identify, prioritize and eliminate the most vital avenues that attackers can exploit.

Specifically administrators can monitor Tier Zero assets for their Active Directory and Azure environment. Tier Zero is the highest level of the Active Directory tiered administrative model and includes administrative accounts, groups, domain controllers, and domains that have direct or indirect administrative control of the Active Directory forest.

On Demand Audit provides built-in searches that allow administrators to create alert-enabled search for historical changes to the Tier Zero objects to ensure real-time monitoring of critical assets.

- Configure a SpecterOps BloodHound Integration
- BloodHound Tier Zero assets built in searches
- Monitoring Audit Health status

Configure a SpecterOps BloodHound Integration

To pair SpecterOps BloodHound Enterprise with On Demand Audit to help provide a comprehensive risk assessment and threat monitoring solution, you need to add a SpecterOps BloodHound configuration.

NOTE:

- To manage a SpecterOps BloodHound Enterprise configuration, you must have the **Can Manage SpecterOps BloodHound Configuration** permission.
- Once the configuration has been added, you can select the three vertical dots in the upper right-corner to refresh the configuration immediately, to edit the alert plan, or to read more about the benefits of integrating with SpecterOps BloodHound Enterprise.
- The configuration connection message details whether the connection the SpecterOps has been successful, and the status of the configuration.

To add a configuration:

1. From the **Configuration** tab, select **Add BloodHound Enterprise** or click the **+** icon.
2. Enter the SpecterOps BloodHound URL, the Permanent Authorization Token (PAT) Token ID, and Key pair.

3. Click **Validate** to validate the URL format (https://yourdomain.bloodhoundenterprise.io.), the Permanent Authorization Token (PAT) Token ID, and the Key pair.
4. Click **Save**.

   Once the configuration has been added, you can select to edit the Tier Zero alert plan to configure who will be notified when an alert is triggered.

To edit a configuration:

1. From the **Configuration** tab, select the BloodHound Enterprise card, and choose **Edit Configuration**.
2. Edit the SpecterOps BloodHound URL, Permanent Authorization Token (PAT) Token ID, and Key pair as required.
3. Click **Validate** to validate the URL format (https://yourdomain.bloodhoundenterprise.io.), the Permanent Authorization Token (PAT) Token ID, and the Key pair.
4. Click **Save**.

To remove a configuration:

> **IMPORTANT:** When you remove a configuration, SpecterOps BloodHound Enterprise information will no longer be added to events in On Demand Audit.

1. From the **Configuration** tab, select the BloodHound Enterprise card, and choose **REMOVE**.
2. Click **YES** to remove the configuration.

6

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. The information is updated in real time, allowing you to quickly gain valuable insights into the activity taking place in your organization. You can also refresh the data by selecting the refresh icon in the top right of the dashboard.

The dashboard displays:

- Activity status indicators. For details, see Working with Activity Indicators
- Audit health status. For details, see Monitoring Audit Health status.
- Azure Active Directory ID sign-in risk events
- Critical activity. For details, see Identifying critical activity.
- Top active users. For details. see Identifying the top active users.
- Favorite searches. For details, see Working with My Favorite Searches.
- Log in trends. For details, see Monitoring sign-in trends.

Working with Activity Indicators

The indicators at the top of the dashboard allow you to quickly see if there has been a change in risky activity over a specific period of time. A red sidebar indicates an increase in activity; while a green sidebar indicates a reduction.

You can then easily delve further into the details, by clicking the indicator to view an associated search.

> **NOTE:** The indicators are updated each time that you open the dashboard or refresh the view.

The following indicators are available:

- Cloud-only Azure Active Directory users created in the last 7 days
- AD account lockouts in the last 24 hours

  If you do not have a configured Change Auditor integration, the Azure Active Directory critical directory role changes in the last 7 days indicator displays instead.
- Azure Active Directory risk events in the last 7 days

  This indicator displays when you have an Azure Active Directory Premium (P2) license.

  If you do not have the required license to audit risky events and Change Auditor integration is configured, the On-premises and Azure Active Directory failed sign-ins in the last 24 hours indicator displays instead.

  If you do not have the required license to audit risky events and have not configured a Change Auditor integration, the Azure Active Directory failed sign-ins in the last 24 hours indicator displays.
- Office 365 external user actions in the last 24 hours

Monitoring Audit Health status

The Audit Health tile allows you to easily see the status of your auditing configuration, identify any issues, and make the required updates to ensure you are keeping informed of the vital and critical changes to your organization.

From here, you can grant required consent for the tenant, view subscription information, view the auditing configuration settings, view results in a search, and subscribe to the built-in alert plans.

> **NOTE:** Specific permissions are required for the following actions:
>
> - Can Add and Remove Tenants is required to grant consent.
> - Can Run Private Searches and Can Run Shared Searches are required to view associated results.
> - Can Manage Azure Active Directory Tenant Configurations for Audit is required to view issues identified for tenants.
> - Can Manage Change Auditor Installation Configuration is required to view issues identified for Change Auditor.
> - Can Manage Shared Alerts and Shared Alert Plans and Can Run Shared Searches is required to subscribe to the alert plans.

NOTE:

- You have the option to hide items from the dashboard if they do not provide you any value, expose previously hidden items, and dismiss notifications as required.
- You have the option to dismiss the ability to subscribe to the available alert plans. Once it has been dismissed, it will no longer be displayed as an option in the Audit Health dashboard.

Possible issues that may be identified include:

- Tenant requires additional configuration
- Tenant has not been added for auditing
- Service subscription will expire soon
- Service is not enabled for event collection on the tenant
- Event collection has been disabled on the tenant
- No Office 365 events have been received from the tenant in the last 24 hours
- No Azure AD events have been received from the tenant in the last 24 hours
- No Azure AD Sign-in events have been received from the tenant in the last 24 hours
- No Change Auditor events have been received in the last 24 hours
- Change Auditor installation has been paused
- Change Auditor installation was removed
- Change Auditor installation has not been connected in the last 24 hours
- Change Auditor upgrade is required
- Change Auditor upgrade is available
- Configure SpecterOps BloodHound Enterprise integration
- SpecterOps BloodHound Enterprise configuration was removed
- SpecterOps BloodHound Enterprise connection failed
- Subscribe to Tier Zero alert plan

To subscribe to an alert plan from the Audit Health tile in the dashboard:

1. Select **View Plan** for the alert plan that you want to subscribe to.
2. Edit the alert recipients as required, and click **Save**.

Identifying critical activity

The Critical Activity tile highlights security-related activity, including anomaly detection for unusual spikes in activity, that may indicate a threat to your organization and require further investigation.

NOTE: Critical activity events are gathered and displayed based on the services that you have selected to audit.

See Configuring tenant auditing for details on selecting services to audit and Change Auditor Integration for details on accessing on premises events.

Audited Service	Critical activity
Change Auditor / Logon Activity	• Local logons to Tier Zero computers • NTLM version 1 logons • Possible Golden Ticket Kerberos exploits • Potential kerberoasting or similar Kerberos attack detected • Tier Zero user logons to computers that are not Tier Zero • Unusual increase in AD account lockouts • Unusual increase in failed on-premises sign-ins • Unusual increase in successful on-premises sign-ins
Change Auditor / Active Directory	• Administrative privilege elevation detected • AD user ServicePrincipalName attribute changes detected • Active Directory critical group membership changes • Active Directory schema configuration changes • Active Directory forest configuration changes • Active Directory security changes • Domain level group policy linked changes detected • Irregular AD replication activity detected • Irregular domain controller registration detected (DCShadow) • Potential sIDHistory injection detected • Security changes to Tier Zero computer objects • Security changes to Tier Zero domain objects • Security changes to Tier Zero group objects • Security changes to Tier Zero group policy objects • Security changes to Tier Zero user objects • Tier Zero computer changes • Tier Zero domain and forest configuration changes • Tier Zero group changes • Tier Zero group policy object changes

Audited Service	Critical activity
	• Tier Zero user changes • Unusual increase in failed AD changes • Unusual increase in permission changes to AD objects
Change Auditor / Active Directory Federation Services	• Unusual increase in successful AD Federation Services sign-ins • Unusual increase in failed AD Federation Services sign-ins
Change Auditor / File System	• AD Database (NTDS.dit) access attempt detected • AD Database (NTDS.dit) file modification attempt detected • All file changes with suspicious file extensions • Unusual increase in share access permission changes • Unusual increase in failed file access attempts • Unusual increase in file deletes • Unusual increase in file renames
Change Auditor / Group Policy	• Group Policy changes
Azure Active Directory - Audit Logs	• Azure Tier Zero application changes • Azure Tier Zero group changes • Azure Tier Zero role changes • Azure Tier Zero service principal changes • Azure Tier Zero tenant level and directory activity • Azure Tier Zero user changes • Azure Active Directory critical directory role changes • Azure Active Directory tenant level configuration changes • Azure Active Directory cloud-only users created
Azure Active Directory - Sign Ins	• Azure Tier Zero principal logons • Azure Tier Zero AD risk events • Unusual increase in tenant sign-in failures • Unusual increase in successful tenant sign-ins
Exchange Online - Administrative Activity	• OneDrive and SharePoint files shared with external users • OneDrive and SharePoint anonymous links • Office 365 activity from external users

Audited Service	Critical activity
Sharepoint Online or OneDrive For Business	• Unusual increase in files shared from OneDrive and SharePoint • Unusual increase in Office 365 activity by guest users • Unusual increase in Office 365 activity by anonymous users
Microsoft Teams	• Unusual increase in Teams guest participants

You can easily dive deeper into the activity by viewing the associated search. For details on the searches associated with the critical activity see Working with searches, Working with Azure Active Directory Searches and Using built in searches.

To view a full list of critical activity as well as visualizations to help understand the possible threat, see Working with critical activity.

Identifying the top active users

The Top Active Users tile displays the top five active users in the last 24 hours with each service represented by a different color bar. By default, data for all available services is displayed.

To view the exact number of events per service for a particular user, hover over a section of the bar. To dive deeper into the activity details, click the section of the bar that represents the service of interest.

> **NOTE** Other than On Demand Audit activity, which will always be included, the activity that is gathered and displayed is based on the services that you have selected to audit.
>
> See Configuring tenant auditing for details on selecting services to audit and Change Auditor Integration for details on accessing on premises events.

Audited Service	Activity
Change Auditor	• Active Directory • Active Directory Federation Services (Change Auditor version 7.1.2 or later) • Active Directory Database • Group Policy • Logon Activity
OneDrive for Business	• OneDrive
SharePoint Online	• SharePoint
Micorosft Teams	• Teams
Azure Active Directory - Audit Logs Azure Active Directory - Sign-ins	• Azure Active Directory

Audited Service	Activity
Exchange Online - Administrative Activity Exchange Online - Mailbox Activity	• Exchange

To view the top active users for a specific service

1. Choose the required service from the dropdown list, and click **Select**.
2. To exclude users from being included in the calculations and display, select the Edit Excluded Users and add and remove users as required.
3. Click **Close** to save your selection.

Working with My Favorite Searches

The My Favorite Searches section of the dashboard allows you to pin the top five searches that you have defined as having a high value in your organization. From here you can see the number of events, select to view the search details, and manage which searches to displayed in this view.

By default, the following searches are listed:

- Important changes for critical Azure Active Directory directory roles in the past 7 days
- Azure Active Directory role member changes in the past 7 days
- Cloud-only Azure Active Directory users created in the past 180 days
- Azure Active Directory tenant level configuration changes in the last 180 days
- Office 365 events from EXT Users in the past 7 days

To manage the searches displayed on the dashboard:

1. From My Favorite Searches, click **Edit Searches**.
2. Add and remove searches as required by selecting the category and associated search. You can also drag and drop to specify the search order on the dashboard based on priority.
3. Once you have made all your selections, click **OK**.

Monitoring sign-in trends

The Sign-ins tile allows you to quickly see the successful and failed sign-ins over the last 7 days. You can select monitor trends for all sign-ins or select only those that you are interested in.

To add and remove the types of sign-in trends displayed:

1. Expand the drop-down list and choose the type of sign-ins to display.
2. Select to show all or successful or failed Azure Active Directory sign-ins, Active Directory authentications, and Windows interactive logons.

If you have selected to show "All" sign-in types, any services added at a later date will automatically be selected and displayed in the dashboard.

NOTE: Sign-in activity is gathered and displayed based on the services that you have selected to audit. See Configuring tenant auditing for details on selecting services to audit and Change Auditor Integration for details on accessing on premises events.

Audited Service	Sign in events
Change Auditor / Logon Activity	• Active Directory authentications - Successful events • Active Directory authentications - Failed events • Windows interactive logons - Successful events • Windows interactive logons - Failed events
Azure Active Directory - Sign-in	• Azure Active Directory sign-ins - Successful events • Azure Active Directory sign-ins - Failed events

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. You can also modify which columns to display and how the content is displayed.

NOTE: The results returned will only include activity from the last 365 days.

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.

To edit the display layout

1. Click **Edit Layout** to rearrange, add, and remove columns as required and select the visualization options.
    a. Using the Columns menu, drag and drop the columns to change the order.
    b. To add a column, click **Add Column.**
    c. To remove a column, click the **-** next to the appropriate column.
    d. Select the Visualize menu ad choose how to visualize the results. You can choose between a **Chart & Grid**, **Grid** only, or **Chart** only. If you select to display as a chart, you can further refine the display by selecting the type of chart and how you want to group and summarize the data.
    e. Click **Preview** when you are satisfied with the edits.

Working with critical activity

The Critical Activity page displays a full list of security-related activity, including anomaly detection for unusual spikes in activity, that may indicate a threat to your organization.

By default, the activity is displayed based on priority from high to low. You can sort and filter the list based on priority, critical activity, and event count and select to hide or remove specific events from the display.

From this page, you can see tailored visualizations and metrics to provide more context about the activity and related search and a high-level overview of the item.

This information helps determine if the activity is expected behavior, an actual issue. Anomaly detection allows you to gain further insight into configuration issues which could impact user experience and service availability and help identify compromised devices or malicious activity.

NOTE:

- Any detected anomalies include an exclamation point in the icon.
- As events are analyzed and the baselines are updated, the data in the charts will update accordingly. Because of this, some items may disappear in the critical activity pane if they no longer are included in the activity spike.
- Anomaly detection depends on the users' a time zone. As a result, users within the same organization may see a different set of anomalies.

To view critical activity and configure the display:

1. Select **Critical Activity**, and click the activity of interest. When you select an activity, a chart displays information by percentage of user, target, or activity or by number of events per target. For anomalies and unusual spikes in activity, the resulting chart displays the baseline (predicted value), anomalies (unusual increase), and total amounts of activity. For all other critical activity the targets associated with the event are displayed in a donut chart. You can select which targets to include in the visualization by selecting (and de-selecting) entries from the legend.
2. Click on any section of the chart for specific search details, or select **View All Events** to see all related searches.

3. If you select a section of the donut chart or a data point on the time series chart for an anomaly, the filtered search will display the associated visualization so that you can quickly view the details of the activity.
4. If required, select **Dismiss Activity** to remove the reported results until the next activity is detected or just select to hide future occurrences of this event.
5. If you have hidden any events and want them added back to the display, select **Edit Hidden Items**, click the events that you want added back to the view, **Remove Selected Items**, and **Save**.
6. To filter the list of critical events, select **Filter**, choose if you want to filter on priority (High, Medium, Low), specific critical activity, or number of events.

Working with searches

Working with private and shared searches

When you create a search, you have the option of selecting whether it will be private or shared.

- Private searches are only visible to the individual who created them.
- Shared searches are visible to all On Demand Audit users and allow for collaboration with multiple users from the same organization.

NOTE:

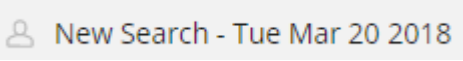
- The ability to set the search type as private or shared depends on your assigned access role within On Demand Audit. For details, see On Demand Audit Access Control roles
- Private search names must be unique among all categories for each user.
- Shared search name must be unique among all shared searches in all categories in the organization
- All private searches (as well a searches under the My Searches category) are listed under the All Private Searches category.
- Shared searches include an information icon that allows you to see when they were created, last saved, and by whom.

See Creating a custom search, Creating a search from an existing search, and Modifying a search

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.
- 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. These are shared searches.

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
- Active Directory Database built in searches
- Active Directory Federation Services built in searches
- Anomaly Activity built in searches
- Audit Health built in searches
- Azure Active Directory built in searches
- Best Practices built in searches
- BloodHound Tier Zero assets built in searches
- File System built in searches
- Group Policy built in searches
- Logon Activity built in searches
- Office 365 built in searches
- On Demand Audit built in searches
- Teams built in searches
- Security Guardian 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.
- 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 adminCount attribute changed events in the past 30 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 inheritance settings changed events in the past 30 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 sIDHistory attribute changed events in the past 30 days
- AD all high severity sIDHistory attribute changed events in the past 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 irregular domain controller registration events in the past 30 days
- AD irregular domain replication detected events in the past 30 days
- AD user ServicePrincipalName attribute changes 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.

Active Directory Federation Services built in searches

On Demand Audit provides the following Active Directory Federation Services built in searches:

- AD FS All claims provider trust events in the past 30 days
- AD FS All relying party trust events in the past 30 days
- AD FS All endpoint events in the past 30 days
- AD FS All authentication method changes in the past 30 days
- AD FS All server farm events in the past 30 days
- AD FS Authentication method registered and unregistered events in the past 30 days

Active Directory Database built in searches

On Demand Audit provides the following Active Directory Database built in search:

- AD DB all events in the past 7 days

Anomaly Activity built in searches

On Demand Audit provides the following anomaly activity built in searches:

- All anomaly detected events in the past 30 days
- Unusual increase in AD account lockout events in the past 30 days
- Unusual increase in failed AD change events in the past 30 days
- Unusual increase in failed AD Federation Services sign-ins in the past 30 days
- Unusual increase in failed file access attempts in the past 30 days
- Unusual increase in file deletes in the past 30 days
- Unusual increase in file renames in the past 30 days
- Unusual increase in files shared from OneDrive and SharePoint events in the past 30 days
- Unusual increase in Office 365 activity by guest user events in the past 30 days
- Unusual increase in Office 365 activity by anonymous user events in the past 30
- Unusual increase in permission changes to AD object events in the past 30 days
- Unusual increase in share access permission changes in the past 30 days
- Unusual increase in successful AD Federation Services sign-ins in the past 30 days
- Unusual increase in successful tenant sign-in events in the past 30 days
- Unusual increase in tenant sign-in failure events in the past 30 days
- Unusual increase in Teams guest participant events in the past 30 days
- Unusual increase in successful on-premises sign-ins in the past 30 days
- Unusual increase in failed on-premises sign-ins in the past 30 days

Audit Health built in searches

On Demand Audit provides the following Audit Health built in searches:

- Change Auditor Installation activity changes in the past 30 days
- Change Auditor Installation connectivity events in the past 30 days
- Change Auditor Installation setting changes in the past 30 days
- Change Auditor Installation upgrade events in the past 30 days
- Service activity changes in the past 30 days
- Service auditing enabled or disabled events in the past 30 days
- SpecterOps BloodHound Enterprise connectivity events in the past 30 days
- SpecterOps BloodHound Enterprise configuration changes in the past 30 days
- Subscription expiring events in the past 90 days

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 searches:

- Azure AD successful application consent events in the past 30 days
- Sharing operations on important file types within past 7 days
- Teams guest access enabled or disabled in the past 30 days

BloodHound Tier Zero assets built in searches

On Demand Audit provides the following BloodHound Tier Zero assets built in searches:

- All Azure Tier Zero AD risk events in the past 60 days
- All Azure Tier Zero application changes in the past 60 days
- All Azure Tier Zero group changes in the past 60 days

- All Azure Tier Zero principal logons in the past 60 days
- All Azure Tier Zero role changes in the past 60 days
- All Azure Tier Zero service principal changes in the past 60 days
- All Azure Tier Zero tenant level and directory activity in the past 60 days
- All Azure Tier Zero user changes in the past 60 days
- All Tier Zero computer changes in the past 60 days
- All Tier Zero domain and forest configuration changes in the past 60 days
- All Tier Zero group changes in the past 60 days
- All Tier Zero group policy item and object changes in the past 60 days
- All Tier Zero user changes in the past 60 days
- Local logons to Tier Zero computers in the past 60 days
- Security changes to Tier Zero domain objects in the past 60 days
- Security changes to Tier Zero group objects in the past 60 days
- Security changes to Tier Zero group policy objects in the past 60 days
- Security changes to Tier Zero computer objects in the past 60 days
- Security changes to Tier Zero user objects in the past 60 days
- Tier Zero user logons to computers that are not Tier Zero in the past 60 days

File System built in searches

On Demand Audit provides the following File System built in searches:

- FS all events in the past 7 days
- FS all permission and ownership changes to SYSVOL on domain controllers in the past 30 days
- FS all local share changes in the past 30 days
- FS all file and folder creates, deletes, and moves in the past 30 days
- FS all file and folder attribute changes, modifications, and renames in the past 30 days
- FS all file and folder auditing changes in the past 30 days
- FS all file and folder ownership changes in the past 30 days
- FS all file and folder permission changes in the past 30 days
- FS all file and folder failed access attempts in the past 30 days
- FS all file changes with suspicious file extensions 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
- Group Policy domain level linked changes in the past 30 days

Logon Activity built in searches

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

- AD FS All Active Directory Federation Services sign-ins in the past 24 hours
- AD FS All Failed Active Directory Federation Services sign-ins in the past 7 days
- AD FS All Successful Active Directory Federation Services sign-ins in the past 24 hours
- 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 Kerberos service tickets created with unsafe encryption type in the past 30 days
- 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

On Demand Audit built in searches

On Demand Audit provides the following On Demand Audit built in searches:

- All On Demand Audit configuration events in the past 30 days
- All On Demand Audit events in the past 30 days
- On Demand Audit alert plan management events in the past 30 days
- On Demand Audit alert ran events in the past 30 days
- On Demand Audit alert rule management events in the past 30 days
- On Demand Audit all shared search and shared category management events in the past 30 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

Security Guardian built in searches

On Demand Audit provides the following Security Guardian built in searches:

- All Security Guardian events in the past 24 hours
- All Security Guardian events in the past 7 days
- SG Detected Anomaly indicators in the past 30 days
- SG Detected TTP indicators in the past 30 days
- SG Hygiene indicators in the past 30 days
- SG Detected Protected indicators in the past 30 days
- SG Tier Zero objects added in the past 30 days
- SG Tier Zero objects removed in the past 30 days
- SG Tier Zero objects certified in the past 30 days
- SG all indicators muted and unmuted in the past 30 days
- SG all objects muted and unmuted in the past 30 days
- SG all Tier Zero objects protected in the past 30 days
- SG all AD DB objects protected in the past 30 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 search display.

NOTE:

- Private search names must be unique among all categories for each user.
- Shared search name must be unique among all shared searches in all categories in the organization

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 search display.
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. Select whether this is a private or shared search. Working with private and shared searches.
8. Click **Save**.
9. 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. Select whether this is a private or shared search. See Working with private and shared searches.
5. 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 search display.
5. Select **Save As**.
6. Edit the search name and select the category.
7. Select whether this is a private or shared search. Working with private and shared searches.
8. Click **Save**.
9. 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 search display

When you create a search, a preview displays to help ensure the search criteria meet your needs. You can easily customizing the columns that display in the generated report and set how you want the report results displayed through the visualization settings.

> **NOTE:** Some columns are included by default, such as Time Detected, User (Actor), Activity, Target, Origin IP, Service, Status, and Tenant Name. For a list of available columns, see Appendix A: Working with search columns and filters

To customize the display of the search results

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 **-** next to the appropriate column.
4. To add a column, click **Add Column.**
5. Select the Visualize menu and choose how to visualize the results. You can choose between a **Chart & Grid**, **Grid** only, or **Chart** only.
6. If you select to display as a chart & Grid or Chart, you can further refine the display by selecting the type of chart (horizontal bar chart, time series, or donut) and how you want to group and summarize the data.
7. Click **Preview** to view your changes.
8. Click **Save** to save your changes.

   If you have selected to visualize the search in a donut or bar chart, you can add and remove items from the display by clicking to clear or enable them from the legend, and select a section of the donut or bar to view more details.

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

You can easily modify a search to gather the information your require as long you have the right to do so.

NOTE:

- Only custom searches can be modified.
- 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. The type of search (private or shared) and the current category is displayed at the top of 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 down list.

5. Click **Edit Columns** to rearrange, add, and remove columns as required and select the visualization options.
    a. Drag and drop the columns to change the order.
    b. To add a column, click **Add Column.**
    c. To remove a column, click the **-** next to the appropriate column.
    d. Select the Visualize menu ad choose how to visualize the results. You can choose between a **Chart & Grid**, **Grid** only, or **Chart** only. If you select to display as a chart, you can further refine the display by selecting the type of chart and how you want to group and summarize the data.
    e. Click **Apply** when you are satisfied with the edits.
6. Select whether this is a private or shared search. Working with private and shared searches.
7. Click **Save** to apply the changes.
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

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

When you create a category, you have the option of selecting whether it will be private or shared.

- Private categories are only visible to the individual who created them.
- Shared categories are visible to all On Demand Audit users and allow for collaboration with multiple users from the same organization.

By default, the following categories are available:

- All Private Searches: All private searches belonging to the signed-in user.
- All Searches: All configured searches.
- Active Directory: All Active Directory events in the last 24 hours, 7 days, and 30 days.
- Active Directory Federation Services: Sign-ins and configuration changes made through Active Directory Federation Services.
- 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.
- Best Practices: Sharing operations on important file types and Teams guest access events.
- Group Policy: Group Policy events.

- Logon Activity: Logon activity events.
- Office 365: Office 365 and SharePoint online events.
- On Demand Audit: All On Demand audit and alert events.
- Teams: Teams user and administrator activity events.
- My searches: A built-in private category.

To create a category

NOTE:

- Private category names must be unique among all categories for each user.
- Shared category name must be unique among all shared searches in all categories in the organization.

1. Under the **Searches** tab, click **Add** in the Categories field.
2. Enter the category name.
3. Select whether the category is private or shared.
4. 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 view you can:

- View the number of alerts created in the last 24 hours for each search.
- View the number of associated alert plans.
- Enable, disable, and remove alerts.
- Add and remove associated alert plans.

- Review searches that have alerts created for them.
- Select an information icon to see when shared alerts were created, last saved, and by whom.

Through the Alert Plans view you can:

- View all the alerts associated with each alert plan and the number of alerts it includes.
- See whether the alert plan it is private (only visible to the individual who created it) or shared (visible to all On Demand Audit users allowing for collaboration with multiple users from the same organization).
- Select an information icon to see when alert plans were created, last saved, and by whom.
- Add, edit, and remove alert plans.

For details, see:

- Managing alerts and alert plans
- Using built in alerts and alert plans

Managing alerts and alert plans

Through alerts you are able to receive detailed information about vital changes and activities as they occur. The associated alert plans allow you to configure who will receive the 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.
- When you create or modify an alert plan, you have the option of selecting whether it will be private or shared.
- When enabling or editing an alert for a private search, only private alert plans can be used or created.
- When enabling or editing an alert for a shared search, only shared alert plans can be used or created.
- An alert plan cannot be removed until all alerts linked to it are removed or reassigned.

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 select whether it will be private or shared. Next, select the link to enter the email recipients for the alert, and click **Save**.

To edit an alert

1. Under the **Alerts** tab, select **Alerts**, select the required alert, and click **Edit Alert**. (You can also edit an alert from the Alert Plans view.)
2. Add and remove the alert plans associate with the alert as required.
    a. To add existing alert plan, select it and click **Save**.
    b. To remove an existing alert plan, clear the check box , and click **Save**.
    c. To create and enable a new alert plan, enter a name for it, and select whether it will be private or shared. Next, select the link to enter the email recipients for the alert, and click **Save**.

To remove an alert

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 plan, and select whether it will be private or shared. Next, select the link to enter the email recipients for the alert, and click **Save**.
4. Click **Send Test** and **OK** to verify that a test alert is sent to the appropriate recipients.

To edit an alert plan

1. Under the **Alerts** tab, select **Alert Plans**, and **Edit Plan**.
2. Edit the alert recipients as required, and click **Save**.

To rename an alert plan

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 plan, and click the **X** icon to delete it.

Using built in alerts and alert plans

On Demand Audit includes built in alerts and alert plans to ensure that you are kept up to date on critical activity within your organization. All searches within the Audit Health, Anomaly Activity, and Bloodhound Tier Zero assets categories are alert-enabled and linked to the associated built in alert plan.

NOTE:

- You must add yourself to the built in alert plan to receive notifications. See Managing alerts and alert plans for details on editing alert plans and alerts.
- Built in alert plans cannot be deleted; you can, however, enable and disable the alerts as required.

The following built in alert plans are available:

- Audit Health
- Anomaly Activity
- Tier Zero

The following built in alerts are available and enabled:

- All anomaly detected events in past 30 days
- All Azure Tier Zero AD risk events in the past 60 days
- All Azure Tier Zero application changes in the past 60 days
- All Azure Tier Zero group changes in the past 60 days
- All Azure Tier Zero principal logons in the past 60 days
- All Azure Tier Zero role changes in the past 60 days
- All Azure Tier Zero service principal changes in the past 60 days
- All Azure Tier Zero tenant level and directory activity in the past 60 days
- All Azure Tier Zero user changes in the past 60 days
- All Tier Zero computer changes in the past 60 days
- All Tier Zero domain and forest configuration changes in the past 60 days
- All Tier Zero group changes in the past 60 days
- All Tier Zero group policy item and object changes in the past 60 days
- All Tier Zero user changes in the past 60 days
- Local logons to Tier Zero computers in the past 60 days
- Security changes to Tier Zero domain objects in the past 60 days
- Security changes to Tier Zero group objects in the past 60 days
- Security changes to Tier Zero group policy objects in the past 60 days
- Security changes to Tier Zero computer objects in the past 60 days
- Security changes to Tier Zero user objects in the past 60 days
- Tier Zero user logons to computers that are not Tier Zero in the past 60 days

- Change Auditor Installation connectivity events in the past 30 days
- Change Auditor Installation setting changes in the past 30 days
- Change Auditor Installation upgrade events in the past 30 days
- Service activity changes in the past 30 days
- Service auditing enabled or disabled events in the past 30 days
- Subscription expiring events in the past 90 days
- Unusual increase in tenant sign-in failure events in the past 30 days
- Unusual increase in AD account lockout events in the past 30 days
- Unusual increase in successful tenant sign-in events in the past 30 days
- Unusual increase in failed AD change events in the past 30 days
- Unusual increase in permission changes to AD object events in the past 30 days
- Unusual increase in files shared from OneDrive and SharePoint events in the past 30 days
- Unusual increase in Office 365 activity by guest user events in the past 30 days
- Unusual increase in Office 365 activity by anonymous user events in the past 30
- Unusual increase in Teams guest participant events in the past 30 days

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 Azure Active Directory Premium (P2) license or higher to audit 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 Active Directory- Audit Log historical events in the last 7 days
Azure Active Directory premium license (Optional)	Azure Active Directory- Audit Log historical events in the last 30 days
Azure Active Directory y premium license (Required)	Azure Active Directory- Sign-ins historical events in the last 30 days
Azure Active Directory Premium license (Required)	Azure Active Directory- 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 • 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)

Audit module	Columns
	• PreviousSignInDateTime (impossible travel risk events only) • PreviousIpAddress (impossible travel risk events only) • PreviousLocation (impossible travel risk events only) • RiskEventDetails • MalwareName • isAtypicalLocation

Working with Azure Active Directory events with multiple targets

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

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

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

Role Event	Target	Subject
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 Active Directory risk event's activity.:

- "New risk event detected" event when the 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 Microsoft 365

On Demand Audit audits activity for Exchange Online, OneDrive for Business, Teams, and SharePoint Online that corresponds to the events in the Microsoft 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
Access Control Policy	• Enter an associated value
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	• Active Directory Federation Services - Server Farm • Active Directory Federation Services - Claims Provider Trusts • Active Directory Federation Services - Authentication Methods • Active Directory Federation Services - Relying Party Trusts • Active Directory Federation Services - Endpoints • AD Query

Filter	Value to enter/ available pre-defined values to select
	• Alert Plan • Alert Rule • Anonymous Cloud Activity • Anonymous Web Site Activity • Audit Configuration • Authentication Activity • Authentication Services Monitoring • Azure Active Directory • Azure Active Directory - Administrative Units • Azure Active Directory - Application • Azure Active Directory - B2B • 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 • Category • Change Auditor Internal Auditing • Computer Monitoring • 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

Filter	Value to enter/ available pre-defined values to select
	• Custom User Monitoring • Defender • Detected Anomaly • Detected Anomaly Item • Detected TTP • Detected TTP Item • 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 • 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 • Full Text Event

Filter	Value to enter/ available pre-defined values to select
	• Group Policy Item • Group Policy Object • Group Monitoring • Hygiene • Hygiene Item • IP Security • Link Configuration • 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 • Search • Security Change Detail • Session Event • Service Monitoring • SharePoint Document • SharePoint Document Library • SharePoint Farm • SharePoint Folder • SharePoint List

Filter	Value to enter/ available pre-defined values to select
	• 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 • Scan Event • SQL Locks Event • SQL Objects Event • SQL OLEDB Event • SQL Performance Event • SQL Progress Report Event • SQL Query Notifications Event • SQL Scan Event • SQL Security Audit Event • SQL Server Event • SQL Session Event • SQL Stored Procedures Event • SQL Transaction Event

Filter	Value to enter/ available pre-defined values to select
	• SQL TSQL Event • SQL User-Configurable Event • Subnets • System Events • SYSVOL • Threat Detection - Alert • Threat Detection - Risky User • TO • TO Item • Transactions Event • 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 • VMware Scheduled Task • VMware Session • VMware Task

Filter	Value to enter/ available pre-defined values to select
	• 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 • App
Affected Items	• Enter an associated value
Agent Domain Fully Qualified Domain Name	• Enter an associated value

Filter	Value to enter/ available pre-defined values to select
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 Plan Name	• Enter an associated value
Alert Plan Type	Select from the following pre-defined values: • Shared Alert Plan • Private Alert Plan
Alert Recipient	• Enter an associated value
Alert Recipients	• Enter an associated value
Alert Rule Name	• Enter an associated value
Alert Rule Type	Select from the following pre-defined values: • Shared Alert Rule • Private Alert Rule
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 Method	• 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

Filter	Value to enter/ available pre-defined values to select
	• V2
Auto Update From Federation Metadata	Select from the following pre-defined values: • Yes • No
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	• Enter an associated value
Browser Authentication URL	• Enter an associated value
Category Name	• Enter an associated value
Category Type	Select from the following pre-defined values: • Shared Category • Private Category
Channel Name	• Enter an associated value
Channel Guid	• Enter an associated value
Channel Type	Select from the following pre-defined valus: • 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
Claims Provider Trust Name	• 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

Filter	Value to enter/ available pre-defined values to select
Comment	• Enter an associated value
Correlated Activity	Select from the following pre-defined values: • Yes • No
Coordinator Id	• Enter an associated value
Correlation Id	• Enter an associated value
Country	• Enter an associated value
Creator	• 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: • 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
Enabled	Select from the following pre-defined values: • Yes • No
Error Code	• Enter an associated value

Filter	Value to enter/ available pre-defined values to select
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
File System Attribute	• Enter an associated value
File System Category	• Enter an associated value
File System Logon Id	• Enter an associated value
File System Object Type	• Enter an associated value
File System Security Change Applies To	• Enter an associated value
File System Security Change Condition	• Enter an associated value
File System Security Change Permission	• Enter an associated value
File System Security Change Type	• Enter an associated value
File System Shadow Copy	• Enter an associated value
File System Share Name	• Enter an associated value
File System SID	• Enter an associated value
First Discovered	• Enter days or hours
Folder	• Enter an associated value
Folder Path	• Enter an associated value
Has file system security change condition	Select from the following pre-defined values: • Yes • No
Has no from value	Select from the following pre-defined values: • Yes

Filter	Value to enter/ available pre-defined values to select
	• No
Identifiers	• Enter an associated value
Indicator	• Enter an assocoated 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
Installation Name	• Enter an associated value
Internal Correlation Id	• Enter an associated value
Is Initial Scan	Select from the following pre-defined values: • Yes • No
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
Latest Activity Time	• Enter the required time frame
Latest Event Time Detected	• Enter the required time frame
Logon Begin 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

Filter	Value to enter/ available pre-defined values to select
	• 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 • Delegated • Delegated Admin • Owner • System Service • Transport • Unknown
Logon Type (Windows)	Select from the following pre-defined values: • None

Filter	Value to enter/ available pre-defined values to select
	• 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
Max Behavior Level	• 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
Modified Properties	• Enter an associated value
Monitor Federation Metadata	Select from the following pre-defined values: • Yes • No
NTLM Impersonation Level	Select from the following pre-defined values: • Default • Anonymous

Filter	Value to enter/ available pre-defined values to select
	• 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 • Account Management: Audit Computer Account Management • Account Management: Audit Distribution Group Management

Filter	Value to enter/ available pre-defined values to select
	• 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 • Audit System Events • Audit: Audit The Access Of Global System Objects • Audit: Audit The Use Of Backup And Restore Privilege

Filter	Value to enter/ available pre-defined values to select
	• 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 • Connection Settings Delete Existing Option • Connection Settings Import Option • Contacts Folder target path • Content Ratings option

Filter	Value to enter/ available pre-defined values to select
	• 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 • Devices: Allow Undock Without Having To Logon • Devices: Allowed To Format And Eject Removable Media • Devices: Prevent Users From Installing Printer Drivers

Filter	Value to enter/ available pre-defined values to select
	• 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 • 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

Filter	Value to enter/ available pre-defined values to select
	• 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 • 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

Filter	Value to enter/ available pre-defined values to select
	• 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 • 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

Filter	Value to enter/ available pre-defined values to select
	• 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 • Modify Firmware Environment • Music Folder options • Music Folder target path • My Documents Folder options • My Documents Folder Redirection: My Pictures Options

Filter	Value to enter/ available pre-defined values to select
	• 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 • 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

Filter	Value to enter/ available pre-defined values to select
	• 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 • 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

Filter	Value to enter/ available pre-defined values to select
	• 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 • 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

Filter	Value to enter/ available pre-defined values to select
	• 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 • Proxy Settings HTTP Proxy • Proxy Settings Secure Proxy • Proxy Settings Socks Proxy • QoS Policy: Application Name • QoS Policy: DSCP Value

Filter	Value to enter/ available pre-defined values to select
	• 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 • Retain System Log • Retention Method For Application Log • Retention Method For Security Log • Retention Method For System Log • Saved Games Folder target path

Filter	Value to enter/ available pre-defined values to select
	• 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 • 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

Filter	Value to enter/ available pre-defined values to select
	• 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 • 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

Filter	Value to enter/ available pre-defined values to select
	• 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 • 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

Filter	Value to enter/ available pre-defined values to select
	• 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 • Registry • Restricted Groups • Scripts (Logon/Logoff) • Scripts (Startup/Shutdown) • Security Levels • Security Options

Filter	Value to enter/ available pre-defined values to select
	• 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
Relying Party Resource	• Enter an associated value
Relying Party Trust Name	• Enter an associated value
Relying Party 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: • Signin • User
Risk Correlation Id	• Enter an associated value

Filter	Value to enter/ available pre-defined values to select
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 • Malware Risk Event • Suspicious IP Risk Event • Unfamiliar Location Risk Event

Filter	Value to enter/ available pre-defined values to select
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
Search Name	• Enter an associated value
Search Type	Select from the follwoing pre-defined values: • Shared Search

Filter	Value to enter/ available pre-defined values to select
	• Private Search
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
Server Farm Name	• Enter an associated value
Server Farm Node Name	• Enter an associated value
Server Farm Node Type	Select from the following pre-defined values: • Primary computer • Secondary computer
Service	Select from the following pre-defined values: • Active Directory • Active Directory Database • Active Directory Federation Services • 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

Filter	Value to enter/ available pre-defined values to select
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 • 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
Subscription Expiry Date	• Enter an associated value
Subscription Name	• Enter an associated value
Subscription Type	• Enter an associated value
Tab Type	• 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

Filter	Value to enter/ available pre-defined values to select
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	Select from the following pre-defined values: • Yes • No
Target is Global Catalog	Select from the following pre-defined values: • Yes • No
Target is Exchange Server	Select from the following pre-defined values: • Yes • No
Target is Tier Zero	Select from the following pre-defined values: • Yes • No
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
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

Filter	Value to enter/ available pre-defined values to select
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 • 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

Filter	Value to enter/ available pre-defined values to select
	• 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
Tier Zero Source	• Enter an associated value
Tier Zero Status	Select from the following pre-defined values: • Certified • Not Tier Zero • Uncertified
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
Url Path	• Enter an associated value
User (Actor)	• Enter an associated value
User Agent	• Enter an associated value

Filter	Value to enter/ available pre-defined values to select
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 is Tier Zero	Select from the following pre-defined values: • Yes • No
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

8

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

Third-party contributions

This product contains the following third-party components. For third-party license information, go to https://www.quest.com/legal/license-agreements.aspx.

For a list of third party contributions for shared services, see the On Demand Global Settings Release Notes.

Table 1: List of Third-Party Contributions

Component	License or Acknowledgement
On Demand Audit Third Party	
Automapper 8.1.1	Use of this component is governed by the MIT 1.0 license. https://github.com/AutoMapper/AutoMapper/blob/master/LICENSE.txt
Angular-resize-event 2.1.0	Use of this component is governed by the MIT license. Copyright (c) 2020 Martin Volek
Azure.Data.Tables 12.7.1	Use of this component is governed by the MIT 1.0 license. Copyright (c) Microsoft Corporation
Azure.Storage.Blobs.Batch 12.14.1	Use of this component is governed by the MIT 1.0 license. Copyright (c) Microsoft Corporation
Azure.Storage.Queues 12.12.0	Use of this component is governed by the MIT 1.0 license. Copyright (c) Microsoft Corporation
Bogus 25.0.4	Copyright 2015 Brian Chavez Copyright 2014-2015 Matthew Bergman & Marak Squires Copyright 2007-2010 Benjamin Curtis Copyright 2004-2005 by Jason Kohles Copyright 2014 - 2016 ZZZ Projects Inc. Copyright 2015 kernys Copyright 2015 Victor Quinn Copyright 2014 Chris Veness Copyright 2013 Richard Morris Copyright 2012 Daniele Faraglia Copyright 2013-2017 Sascha Droste All rights reserved.
Copyright © 2018 Software Freedom Conservancy.Support 3.141.0	Use of this component is governed by the Apache 2.0 license. Copyright © 2018 Software Freedom Conservancy
CsvHelper 12.1.2	Dual licensing under MS-PL and Apache 2.0 1.0 Copyright © 2009-2019 Josh Close and Contributors
Fluent Assertion 5.7.0	Use of this component is governed by the Apache 2.0 license. Copyright Notice - Fluent Assertion 5.7.0
FluentValidation 8.4.0	Use of this component is governed by the Apache 2.0 license. Copyright Notice - FluentValidation 8.4.0 Apache
Google.Protobuf 3.21.6	BSD 3-Clause Template 2020
GraphQL.Client 6.0.1	Use of this component is governed by the MIT 1.0 license.
GraphQL.Client.Serializer 6.0.1	Use of this component is governed by the MIT 1.0 license.
Mailosaur 5.0.14	Use of this component is governed by the MIT 1.0 license. Copyright (c) 2019 Mailosaur Ltd (https://mailosaur.com)
Microsoft Azure Active Directory Graph Client Library 2.1.1	MICROSOFT SOFTWARE LICENSE TERMS - Microsoft Net Library UPDATED 1.0 Copyright © Microsoft Corporation

Component	License or Acknowledgement
	Note: To the extent Microsoft is a processor or sub-processor of personal data in connection with the software, Microsoft makes the commitments in the European Union General Data Protection Regulation Terms of the Online Services Terms to all customers effective May 25, 2018, at http://go.microsoft.com/?linkid=9840733.
Microsoft.ApplicationInsights 2.8.1	Use of this component is governed by the MIT 1.0 license. Copyright (c) Microsoft Corporation
Microsoft.ApplicationInsights.Web 2.4.0	Use of this component is governed by the MIT 1.0 license. Copyright (c) Microsoft Corporation
Microsoft.AspNetCore.WebUtilities 2.2.0	Use of this component is governed by the MIT 1.0 license. Copyright (c) .NET Foundation and Contributors
Microsoft.Azure.ConfigurationManager 4.0.0	Use of this component is governed by the MIT 1.0 license. Copyright (c) 2018 Microsoft
Microsoft.Azure.Cosmos 3.3.1.0	Use of this component is governed by the MIT 1.0 license.
Microsoft.Azure.Devices.Client 1.41.3	Use of this component is governed by the MIT 1.0 license. - Microsoft Azure IoT SDK 1.0 Copyright (c) Microsoft Corporation
Microsoft.Azure.DocumentDB 2.5.1	Use of this component is governed by the MIT 1.0 license. Copyright (c) 2014 Microsoft Corporation
Microsoft.Azure.DocumentDB.Core 2.5.1	Use of this component is governed by the MIT 1.0 license. Copyright (c) 2014 Microsoft Corporation
Microsoft.Azure.EventGrid 2.0.0	Use of this component is governed by the MIT 1.0 license. Copyright (c) 2015 Microsoft
Microsoft.Azure.KeyVault.Core 1.0.0	Use of this component is governed by the Apache 2.0 license. Copyright (c) Microsoft Corporation
Microsoft.Azure.KeyVault.Core 2.0.4	Use of this component is governed by the MIT 1.0 license. Copyright (c) Microsoft Corporation
Microsoft.Azure.Search 5.0.3	Use of this component is governed by the MIT 1.0 license. Copyright (c) 2018 Microsoft
Microsoft.Azure.WebJobs.Extensions 3.0.2	Use of this component is governed by the MIT 1.0 license. Copyright (c) 2018 Microsoft
Microsoft.Azure.WebJobs.Extensions.DurableTask 1.8.3	Use of this component is governed by the MIT 1.0 license. Copyright (c) .NET Foundation. All rights reserved.
Microsoft.Azure.WebJobs.Extensions.EventGrid 2.0.0	Use of this component is governed by the MIT 1.0 license. Copyright (c) .NET Foundation. All rights reserved.
Microsoft.Azure.WebJobs.Extensions.Http 3.0.2	Use of this component is governed by the MIT 1.0 license. Copyright (c) .NET Foundation. All rights reserved.
Microsoft.Azure.WebJobs.Extensions.Storage 5.0.1	Use of this component is governed by the MIT 1.0 license. Copyright (c) Microsoft Corporation
Microsoft.Azure.WebJobs.Extensions.Storage.Blobs 5.0.1	Use of this component is governed by the MIT 1.0 license. Copyright (c) Microsoft Corporation

Component	License or Acknowledgement
Microsoft.Azure.WebJobs.Extensions.Tables 1.0.0	Use of this component is governed by the MIT 1.0 license. Copyright (c) Microsoft Corporation
Microsoft.Extensions.Azure 1.6.0	Use of this component is governed by the MIT 1.0 license. Copyright (c) Microsoft Corporation
Microsoft.Extensions.Caching.Abstractions 2.2.0	Use of this component is governed by the Apache 2.0 license. Copyright (c) .NET Foundation and Contributors
Microsoft.Extensions.Caching.Memory 2.2.0	Use of this component is governed by the Apache 2.0 license. Copyright (c) .NET Foundation and Contributors
Microsoft.Extensions.DependencyInjection 2.2.0	Use of this component is governed by the Apache 2.0 license. Copyright (c) .NET Foundation and Contributors
Microsoft.Extensions.DependencyInjection.Abstractions 2.2.0	Use of this component is governed by the Apache 2.0 license. Copyright (c) .NET Foundation and Contributors
Microsoft.Extensions.Logging 2.2.0	Use of this component is governed by the Apache 2.0 license. Copyright (c) .NET Foundation and Contributors
Microsoft.Extensions.Logging.Abstractions 2.2.0	Use of this component is governed by the Apache 2.0 license. Copyright (c) .NET Foundation and Contributors
Microsoft.IdentityModel.Clients.ActiveDirectory 4.5.1	Use of this component is governed by the MIT 1.0 license. Copyright (c) Microsoft Corporation
Microsoft.IdentityModel.Protocols.OpenIdConnect 5.5.0	Use of this component is governed by the MIT 1.0 license. Copyright Microsoft Corporation. All rights reserved. .
Microsoft.NET.Sdk.Functions 1.0.29	Use of this component is governed by the MIT 1.0 license. Copyright Microsoft Corporation. All rights reserved.
Microsoft.NET.Sdk.Functions 4.1.3	Use of this component is governed by the MIT 1.0 license. Copyright Microsoft Corporation. All rights reserved.
Microsoft.PowerBI.Api 2.0.14	Use of this component is governed by the MIT 1.0 license. Copyright Microsoft Corporation. All rights reserved.
Microsoft.PowerShell.3.ReferenceAssemblies 1.0.0	Use of this component is governed by the MIT 1.0 license. Copyright Microsoft Corporation. All rights reserved.
Microsoft.Rest.ClientRuntime 2.3.20	Use of this component is governed by the MIT 1.0 license. Copyright (c) 2018 Microsoft
Microsoft.Rest.ClientRuntime.Azure 3.3.6	Use of this component is governed by the MIT 1.0 license. Copyright (c) Microsoft Corporation
Microsoft.Web.WebView2 1.0.1343.22	Microsoft.Web.WebView2 1.0 Copyright (C) Microsoft Corporation. All rights reserved.
Microsoft.WindowsAzure.ConfigurationManager 3.2.3	Use of this component is governed by the Apache 2.0 license. Copyright (c) Microsoft Corporation
Moq 4.2.0	Use of this component is governed by the BSD 3 Clause Template 2020 license
Newtonsoft.Json 9.01	Use of this component is governed by the MIT 1.0 license. Copyright (c) 2007 James Newton-King
Newtonsoft.Json.Net 13.0.1	Use of this component is governed by the MIT 1.0 license.

Component	License or Acknowledgement
Polly 6.1.2	Copyright (c) 2007 James Newton-King BSD - Polly 7.1license Copyright (c) 2015-2017, App vNext
Selenium.Support 3.141.0	Use of this component is governed by the Apache 2.0 license. Copyright © 2019 Software Freedom Conservancy
SeleniumExtras.WaitHelpers 3.11.0	Use of this component is governed by the Apache 2.0 license. Copyright 2018, Software Freedom Conservancy
Serilog 2.8.0	Use of this component is governed by the Apache 2.0 license. Copyright Serilog Contributors
Serilog.Extensions.Logging 1.4.0	Use of this component is governed by the Apache 2.0 license. https://github.com/serilog/serilog-extensions-logging/blob/dev/LICENSE
Serilog.Sinks.AzureTableStorage 4.0.0	Use of this component is governed by the Apache 2.0 license. http://www.apache.org/licenses/LICENSE-2.0 Apache
SpecFlow 2.4.1	Licence (New BSD License) 2.1 Copyright (c) 2009, TechTalk SpecFlow
System.CodeDom 4.5.0	Use of this component is governed by the MIT 1.0 license. Copyright (c) .NET Foundation and Contributors
System.Drawing.Common 4.7.2	Use of this component is governed by the MIT 1.0 license.
System.IdentityModel.Tokens.Jwt 5.1.5	Use of this component is governed by the MIT 1.0 license. Copyright (c) Microsoft Corporation. All rights reserved
System.Net.Https 4.3.1	Copyright (c) Microsoft Corporation. All rights reserved
System.Text.RegularExpressions 4.3.1	Copyright ©.NET Foundation. All Rights reserved.
WindowsAzure.Storage 7.2.1	Use of this component is governed by the Apache 2.0 license. Copyright (c) 2013 Microsoft Corp
WindowsAzure.Storage 9.3.1	Use of this component is governed by the Apache 2.0 license. © Microsoft Corporation. All rights reserved.