ONESEC

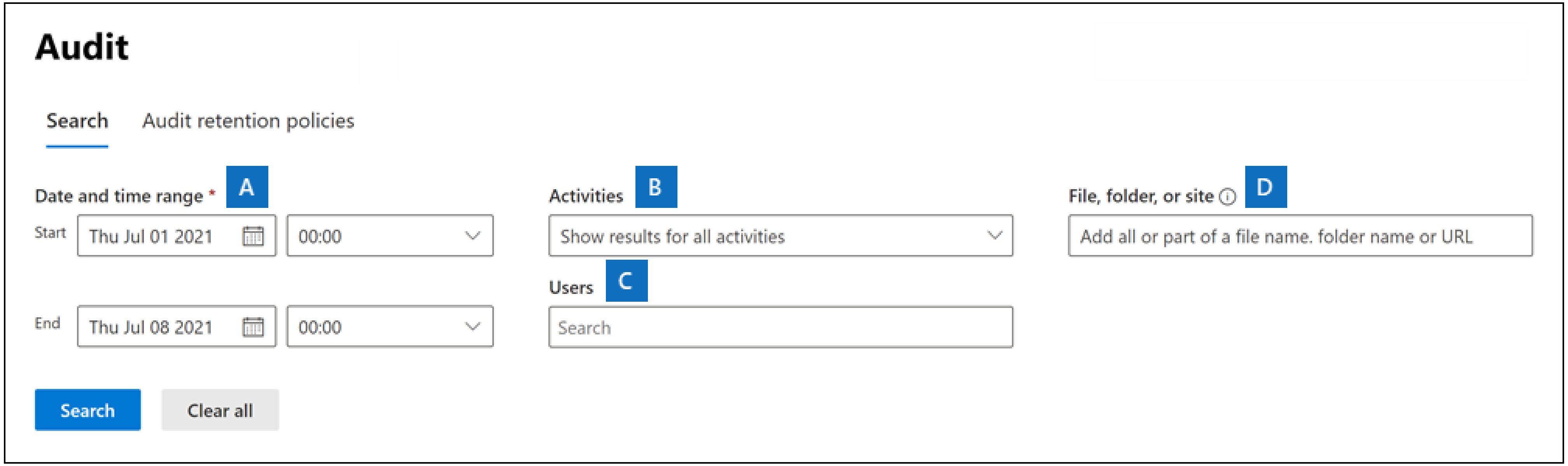
ALWAYS SECURE, *NEVER AT RISK*

Onesec Identity Governance Lifecycle Assessment

ONESEC

Audit logs in the Microsoft Purview Compliance Portal

You can use the audit log search tool in Microsoft Purview compliance portal to search the unified audit log to view user and administrator activity in your organization. Thousands of user and admin operations performed in dozens of Microsoft 365 services and solutions are captured, recorded, and retained in your organization's unified audit log. Users in your organization can use the audit log search tool to search for, view, and export (to a CSV file) the audit records for these operations.



Audit

Date and time range *

Start: Thu Jul 01 2021 — 00:00

End: Thu Jul 08 2021 — 00:00

Activities: Show results for all activities

Users: Search

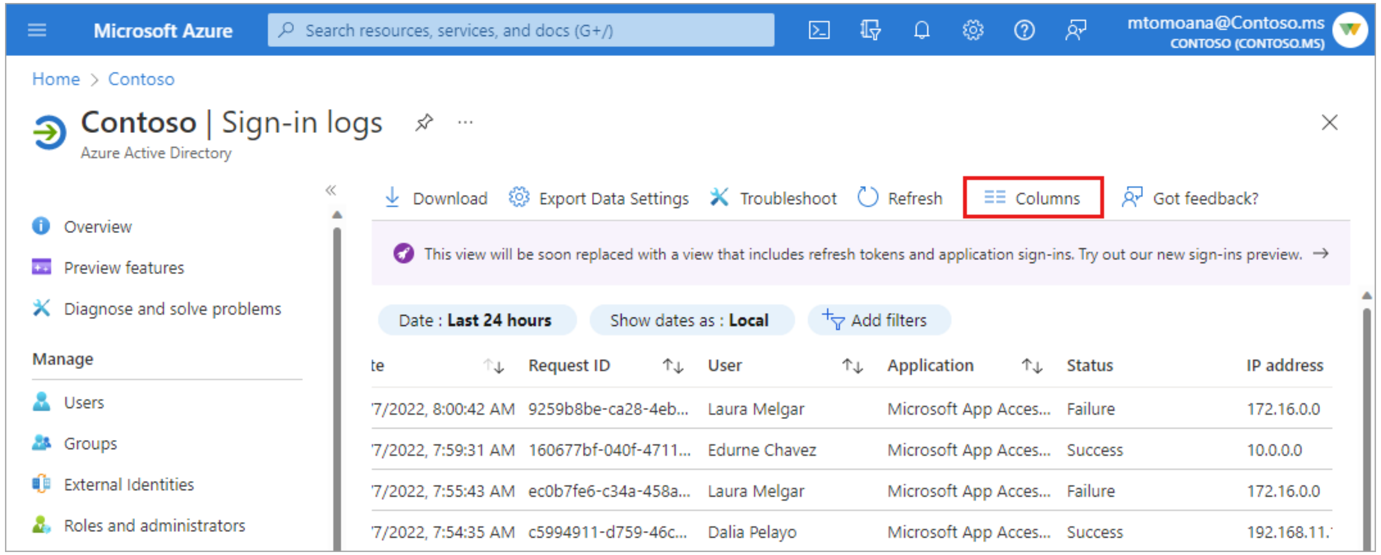
File, folder, or site: Add all or part of a file name. folder name or URL

Sign-in logs in Azure Active Directory

Reviewing sign-in errors and patterns provides valuable insight into how your users access applications and services. The sign-in logs provided by Azure Active Directory (Azure AD) are a powerful type of activity log that IT administrators can analyze.

You can use the sign-ins log to find answers to questions like:

- What is the sign-in pattern of a user?
- How many users have signed in over a week?
- What’s the status of these sign-ins?



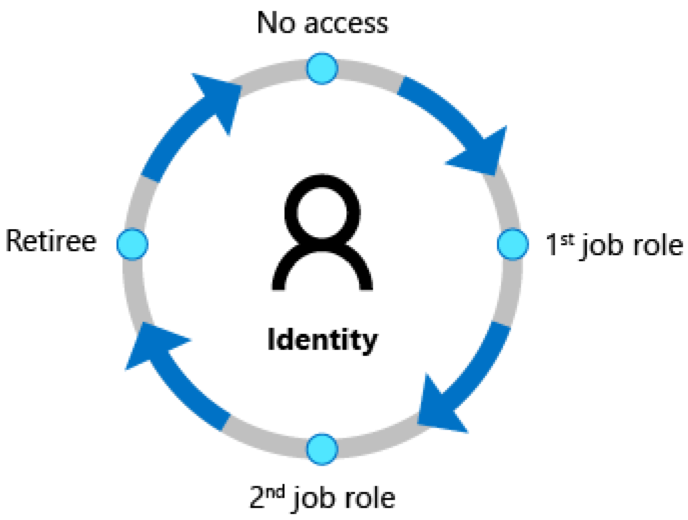
This view will be soon replaced with a view that includes refresh tokens and application sign-ins. Try out our new sign-ins preview. →

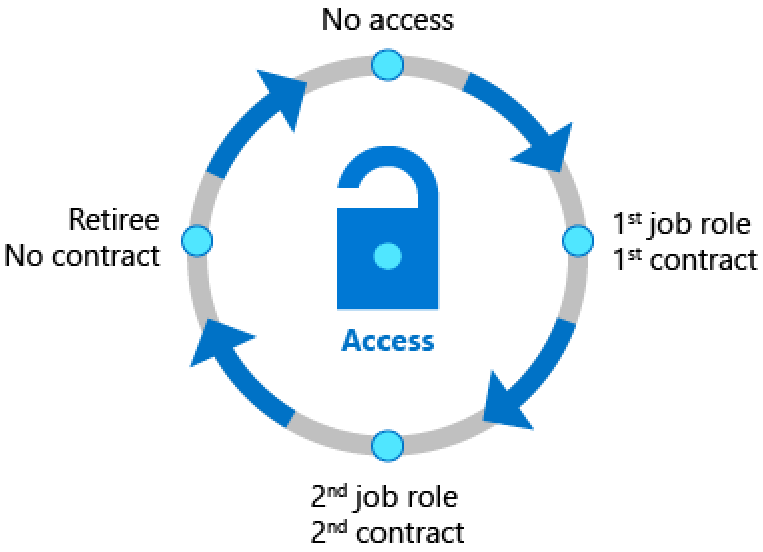
Date : **Last 24 hours**

Show dates as : **Local**

te	Request ID	User	Application	Status	IP address
'7/2022, 8:00:42 AM	9259b8be-ca28-4eb...	Laura Melgar	Microsoft App Acces...	Failure	172.16.0.0
'7/2022, 7:59:31 AM	160677bf-040f-4711...	Edurne Chavez	Microsoft App Acces...	Success	10.0.0.0
'7/2022, 7:55:43 AM	ec0b7fe6-c34a-458a...	Laura Melgar	Microsoft App Acces...	Failure	172.16.0.0
'7/2022, 7:54:35 AM	c5994911-d759-46c...	Dalia Pelayo	Microsoft App Acces...	Success	192.168.11.

Assessment Service





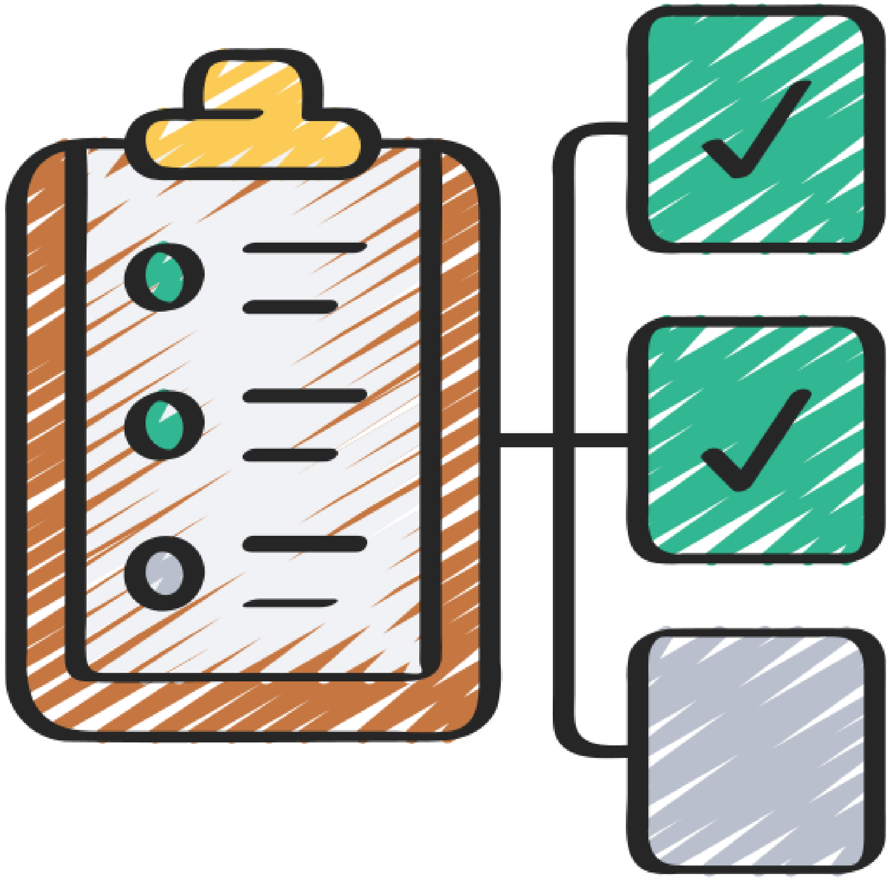
The Assessment of the Onesec Identity Governance Lifecycle has the objective of evaluating the level of Maturity of the Identity Governance Model of organizations, through the analysis of assignments and access logs, carrying out a thorough evaluation of their current identity and access environment and their business requirements to identify deficiencies and detect current risks in the assignment of roles and permissions in your organization.

The Assessment has a duration between 80 and 120 hours and will result in a technical and strategic report on the maturity position of the current identity governance model, as well as a design document and structure of roles and personalized permissions to gradually adopt a Zero Trust environment.

Assessment Deliverables

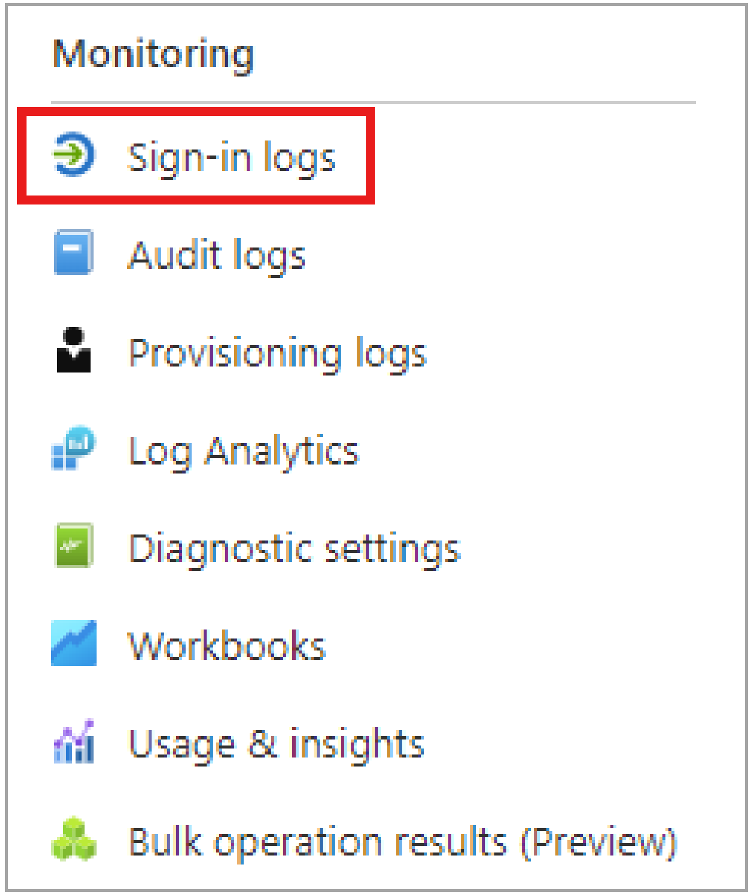
- Technical and strategic report on the maturity position of the current identity governance model: This report will show organizations' current stance on the balance between productivity (how quickly a person can gain access to the resources they need, for example, when they join an organization) and security (how that person's access should change over time, for example, when your employment status changes) of the identities

- Design document and structure of roles and personalized permissions to gradually adopt a Zero Trust environment: Based on a comprehensive assessment of your current identity and access environment, as well as your business requirements, we will design a custom role and permissions structure for your Zero Trust environment.



Licensing and Permissions Requirements

- Licensing requirements for Audit Logs
  - Microsoft Business Basic/Standard subscriptions
  - Microsoft 365 Apps for Business subscription
  - Microsoft 365 Enterprise E3 subscription
  - Microsoft 365 Business Premium
  - Microsoft 365 Education A3 subscription
  - Microsoft 365 Government G1/G3 subscriptions
  - Microsoft 365 Frontline F1 or F3 subscription, or F5 Security add-on
  - Office 365 Enterprise E1/E3 subscription
  - Office 365 Education A1/A3 subscriptions
- The sign-in activity report is available in all editions of Azure AD.
  - To access the sign-ins log for a tenant, you must have one of the following roles:
    - Global Administrator
    - Security Administrator
    - Security Reader
    - Global Reader
    - Reports Reader


Monitoring
Sign-in logs
Audit logs
Provisioning logs
Log Analytics
Diagnostic settings
Workbooks
Usage & insights
Bulk operation results (Preview)