







Audit log search







- Need to find if a user viewed a specific document or purged an item from their mailbox?
- You can use the audit log search tool in Microsoft 365 compliance center 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.

- You have to be assigned the View-Only Audit Logs or Audit Logs role in Exchange Online to search the audit log.
- By default, these roles are assigned to the Compliance Management and Organization Management role groups on the **Permissions** page in the Exchange admin center.
- Global administrators in Office 365 and Microsoft 365 are automatically added as members of the Organization Management role group in Exchange Online.
- To give a user the ability to search the audit log with the minimum level of privileges, you can create a custom role group in Exchange Online, add the View-Only Audit Logs or Audit Logs role, and then add the user as a member of the new role group


 Microsoft 365 admin center







 Settings
 Setup
 Reports
 Health

Admin centers

 Security
 Compliance
 Endpoint Manager
 Azure Active Directory
 Exchange
 SharePoint

<https://security.microsoft.com/?rfr=AdminCenter>


 Microsoft 365 Defender

 Campaigns
 Threat tracker
 Exchange message trace
 Attack simulation training
 Policies & rules

Reports
Audit
Health
Permissions & roles
Settings

More resources

Audit

 [Learn about audit](#)

Search Audit retention policies


 **Start recording user and admin activity**

Date and time range *

Start 1 Ma...  00:00 

End Thu Ma...  00:00 

Activities

Show results for all activities 

Users

Search

File, folder, or site ⓘ


Add all or part of a file name, folde...

Search

Clear all



Audit

 [Learn about audit](#)

Search Audit retention policies

Date and time range *

Start

Thu Mar 17 2022 


00:00 

End


Thu Mar 17 2022 


00:00 

Activities

Deleted file from recycle bin 

Users

 MW

Myrl Whitney 

Search

File, folder, or site ⓘ

test

Search

Clear all

Thursday, Mar 17, 2022 12:00:00 AM to Thursday, Mar 17, 2022 12:00:00 AM

↓

Export

▼

0 items

Date ↓	IP Address	User	Activity	Item	Detail
--------	------------	------	----------	------	--------

- Date:** The date and time (in your local time) when the event occurred.
- IP address:** The IP address of the device that was used when the activity was logged. The IP address is displayed in either an IPv4 or IPv6 address format.
- User:** The user (or service account) who performed the action that triggered the event.
- Activity:** The activity performed by the user. This value corresponds to the activities that you selected in the **Activities** drop down list. For an event from the Exchange admin audit log, the value in this column is an Exchange cmdlet.
- Item:** The object that was created or modified as a result of the corresponding activity. For example, the file that was viewed or modified or the user account that was updated. Not all activities have a value in this column.
- Detail:** Additional information about an activity. Again, not all activities have a value

View the details for a specific event

You can view more details about an event by clicking the event record in the list of search results. A flyout page is displayed that contains the detailed properties from the event record. The properties that are displayed depend on the service in which the event occurs.