Microsoft
CERTIFIED
EXPERT

# Enabling Microsoft Purview Auditing: Permissions + Setup

This project demonstrates how to enable and validate Microsoft Purview auditing, including permissions, setup, and verification steps.

PerparimLabs

#MicrosoftPurview #Auditing #Compliance #PerparimLabs #AzureSecurity

# Why It Matters

Auditing is critical for compliance, investigations, and governance

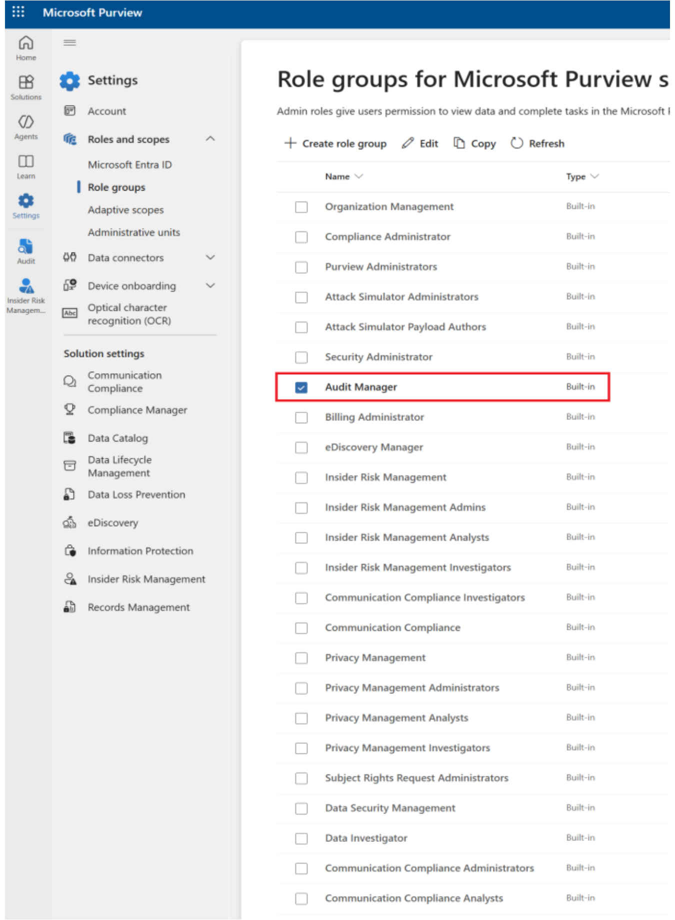
Requires the right **role assignments** + **feature activation**

Without enabling, audit logs will not capture user/admin activity

#MicrosoftPurview #Auditing #Compliance #PerparimLabs #AzureSecurity

# Assigning Permissions

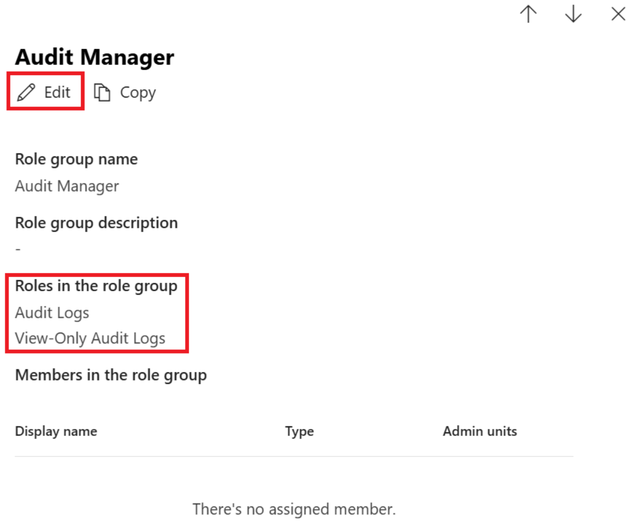
- Go to **Microsoft Purview → Roles and Scopes → Permissions**
- Select **Audit Manager role**
- Role provides:
  - Audit log capability permissions
  - View audit log permissions
- Assign to **users or groups** (e.g., Security Team, Compliance Officer)



## Role groups for Microsoft Purview s

Admin roles give users permission to view data and complete tasks in the Microsoft I

| | Name | Type |
|---|---|---|
| □ | Organization Management | Built-in |
| □ | Compliance Administrator | Built-in |
| □ | Purview Administrators | Built-in |
| □ | Attack Simulator Administrators | Built-in |
| □ | Attack Simulator Payload Authors | Built-in |
| □ | Security Administrator | Built-in |
| ☑ | Audit Manager | Built-in |
| □ | Billing Administrator | Built-in |
| □ | eDiscovery Manager | Built-in |
| □ | Insider Risk Management | Built-in |
| □ | Insider Risk Management Admins | Built-in |
| □ | Insider Risk Management Analysts | Built-in |
| □ | Insider Risk Management Investigators | Built-in |
| □ | Communication Compliance Investigators | Built-in |
| □ | Communication Compliance | Built-in |
| □ | Privacy Management | Built-in |
| □ | Privacy Management Administrators | Built-in |
| □ | Privacy Management Analysts | Built-in |
| □ | Privacy Management Investigators | Built-in |
| □ | Subject Rights Request Administrators | Built-in |
| □ | Data Security Management | Built-in |
| □ | Data Investigator | Built-in |
| □ | Communication Compliance Administrators | Built-in |
| □ | Communication Compliance Analysts | Built-in |



**Audit Manager**

Role group name
Audit Manager

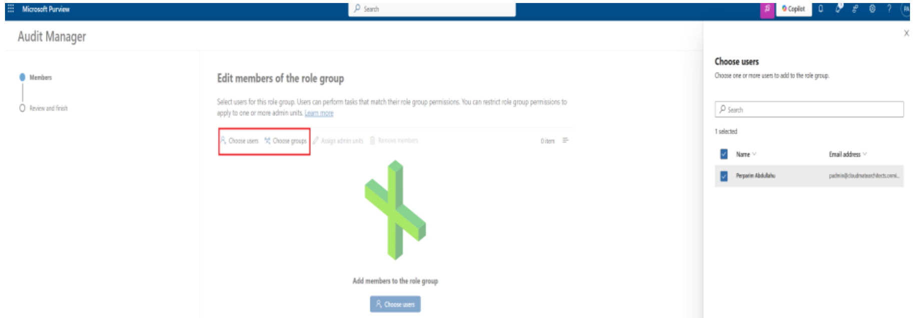
Role group description
-

Roles in the role group
Audit Logs
View-Only Audit Logs

Members in the role group

| Display name | Type | Admin units |
|---|---|---|

There's no assigned member.



Audit Manager

Edit members of the role group

Select users for this role group. Users can perform tasks that match their role group permissions. You can restrict role group permissions to apply to one or more admin units. Learn more

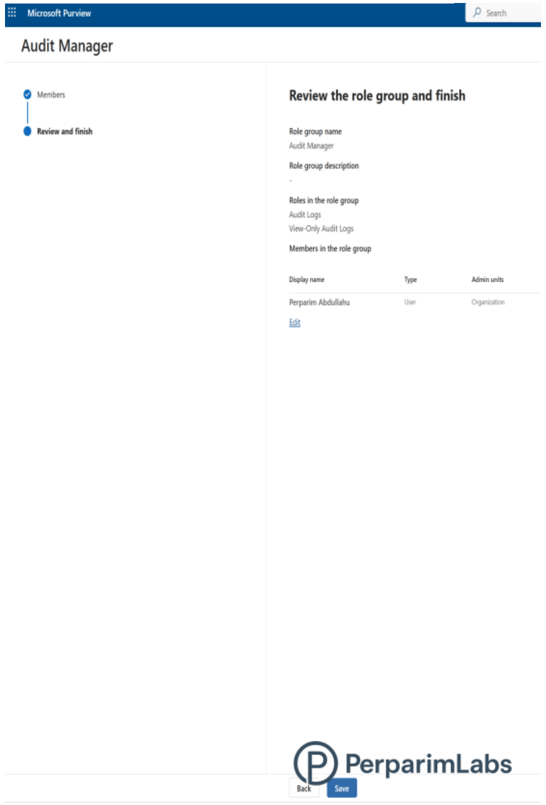
Add members to the role group

Choose users

Choose one or more users to add to the role group.

1 selected

| | Name | Email address |
|---|---|---|
| ☑ | Perparim Abdullahu | padmin@cloudmatearchitects.comi... |



Audit Manager

Review the role group and finish

Role group name
Audit Manager

Role group description
-

Roles in the role group
Audit Logs
View-Only Audit Logs

Members in the role group

| Display name | Type | Admin units |
|---|---|---|
| Perparim Abdullahu | User | Organization |

Edit

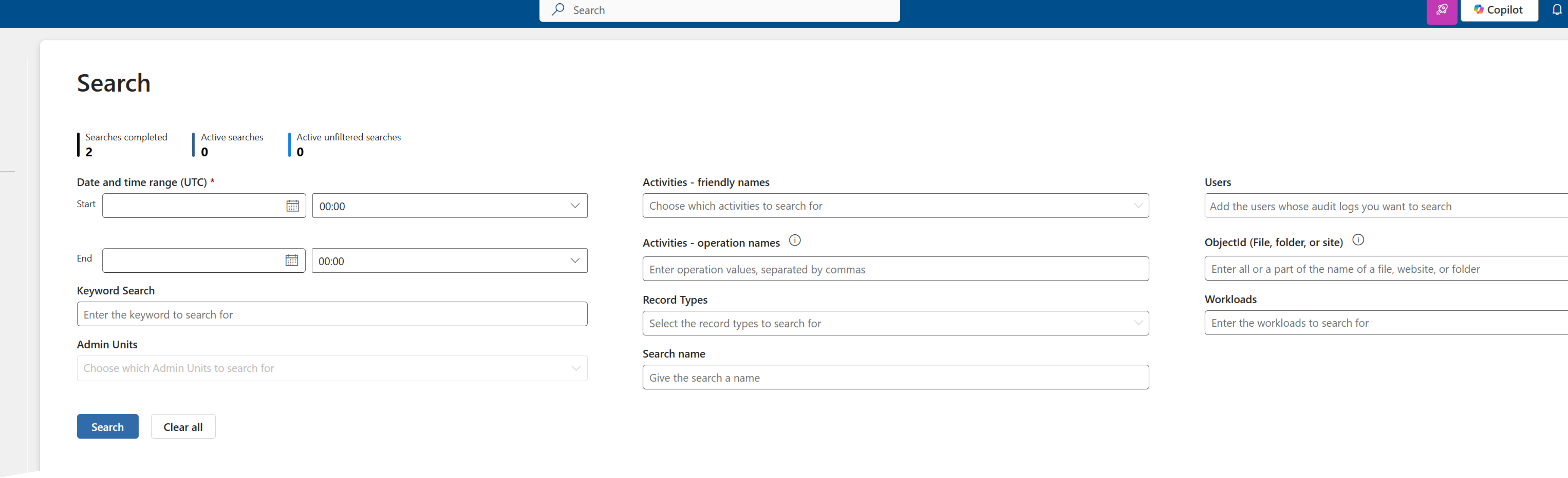
PerparimLabs

#MicrosoftPurview #Auditing #Compliance #PerparimLabs #AzureSecurity

# Enabling Auditing

- First-time users will see **“Start recording user and admin activity”** button
- If already enabled → auditing runs by default
- Changes may take up to **60 minutes** to apply

#MicrosoftPurview #Auditing #Compliance #PerparimLabs #AzureSecurity



Search

Searches completed 2 | Active searches 0 | Active unfiltered searches 0

Date and time range (UTC) *
Start: 00:00
End: 00:00

Keyword Search: Enter the keyword to search for

Admin Units: Choose which Admin Units to search for

Activities - friendly names: Choose which activities to search for

Activities - operation names: Enter operation values, separated by commas

Record Types: Select the record types to search for

Search name: Give the search a name

Users: Add the users whose audit logs you want to search

ObjectId (File, folder, or site): Enter all or a part of the name of a file, website, or folder

Workloads: Enter the workloads to search for

# Validating Audit Logs in Microsoft Purview

- Enabled unified audit logging in **Microsoft Purview**
- Assigned roles & ensured E5 licensing covers audit features
- Performed activity logging with **two test users**
- Ran audit log searches → confirmed **completed queries** show in portal
- Provides visibility into user/admin actions across workloads

#MicrosoftPurview #Auditing #Compliance #PerparimLabs #AzureSecurity

PerparimLabs

# PowerShell Method

- Connect to **Exchange Online PowerShell**

- Check if enabled:

```
Get-AdminAuditLogConfig
```

- Enable auditing:

```
Set-AdminAuditLogConfig -UnifiedAuditLogIngestionEnabled $true
```

# Licensing Reminder

- Users being audited must have valid license:
  - **E3 → Standard auditing =** 90-day retention
  - **E5 → Premium auditing =** up to 10 years with retention policies
- Logs may take time before events appear

# Lab / Industry Example

- In a tenant onboarding project, we enabled auditing by assigning the **Audit Manager role** to the Security team and verified ingestion with PowerShell. This ensured compliance teams could **track privileged admin activity from day one,** aligning with regulatory requirements.

#MicrosoftPurview #Auditing #Compliance #PerparimLabs #AzureSecurity

# Key Takeaways

- Assign **Audit Manager role** before using Purview auditing
- Enable auditing via portal or PowerShell (Set-AdminAuditLogConfig)
- Licenses (E3/E5) determine available features
- Always allow time (up to 60 min) before logs appear

#MicrosoftPurview #Auditing #Compliance #PerparimLabs
#AzureSecurity