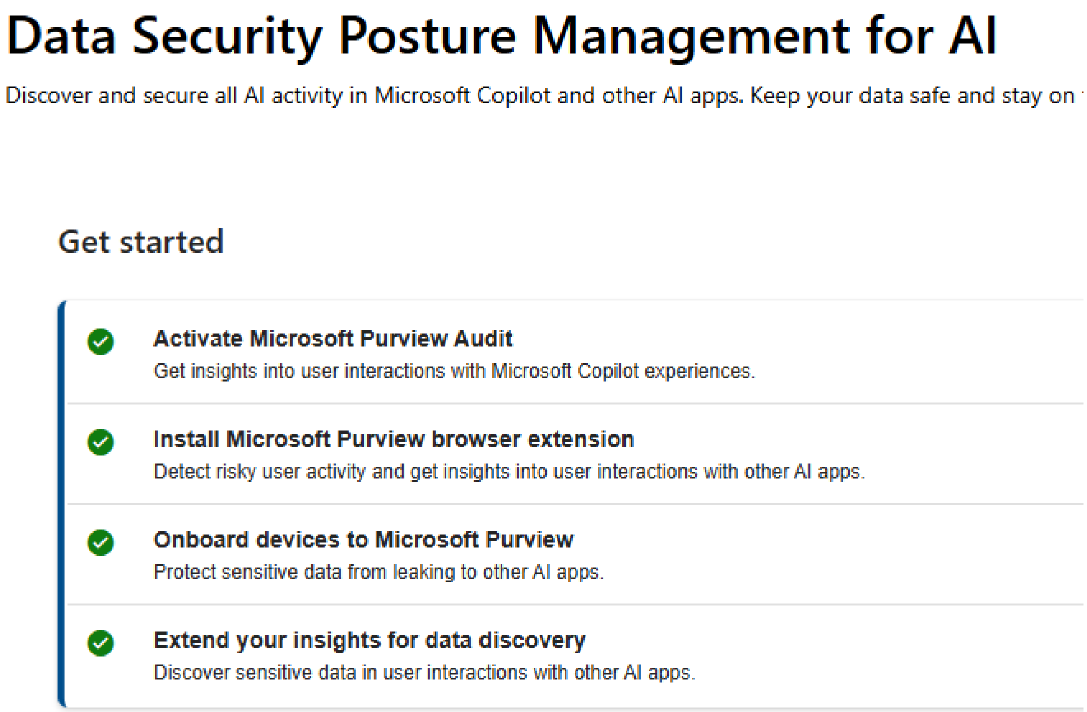
It appears we have met all the pre-reqs:



Data Security Posture Management for AI

Discover and secure all AI activity in Microsoft Copilot and other AI apps. Keep your data safe and stay on

Get started

✓ **Activate Microsoft Purview Audit**
Get insights into user interactions with Microsoft Copilot experiences.

✓ **Install Microsoft Purview browser extension**
Detect risky user activity and get insights into user interactions with other AI apps.

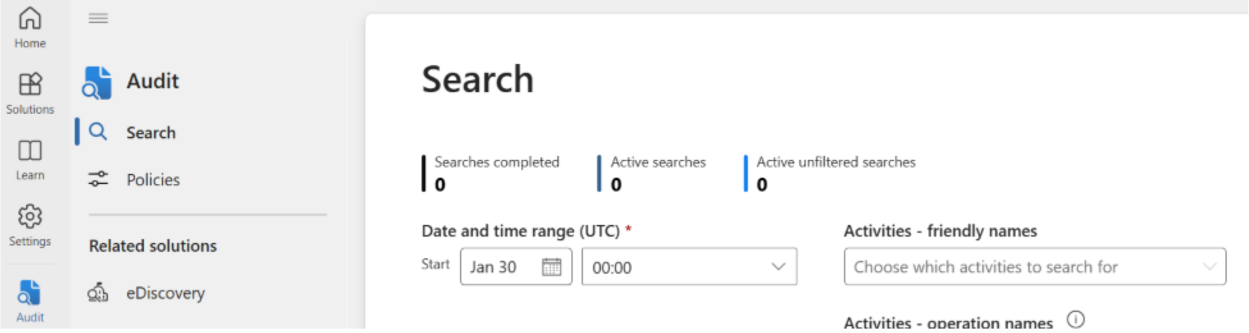
✓ **Onboard devices to Microsoft Purview**
Protect sensitive data from leaking to other AI apps.

✓ **Extend your insights for data discovery**
Discover sensitive data in user interactions with other AI apps.

Pre-requisite 1: Microsoft Purview Activation:

Evidence that Microsoft Purview Audit is enabled:

1 Audit Search available in Purview:



Search

Searches completed
0

Active searches
0

Active unfiltered searches
0

Date and time range (UTC) *

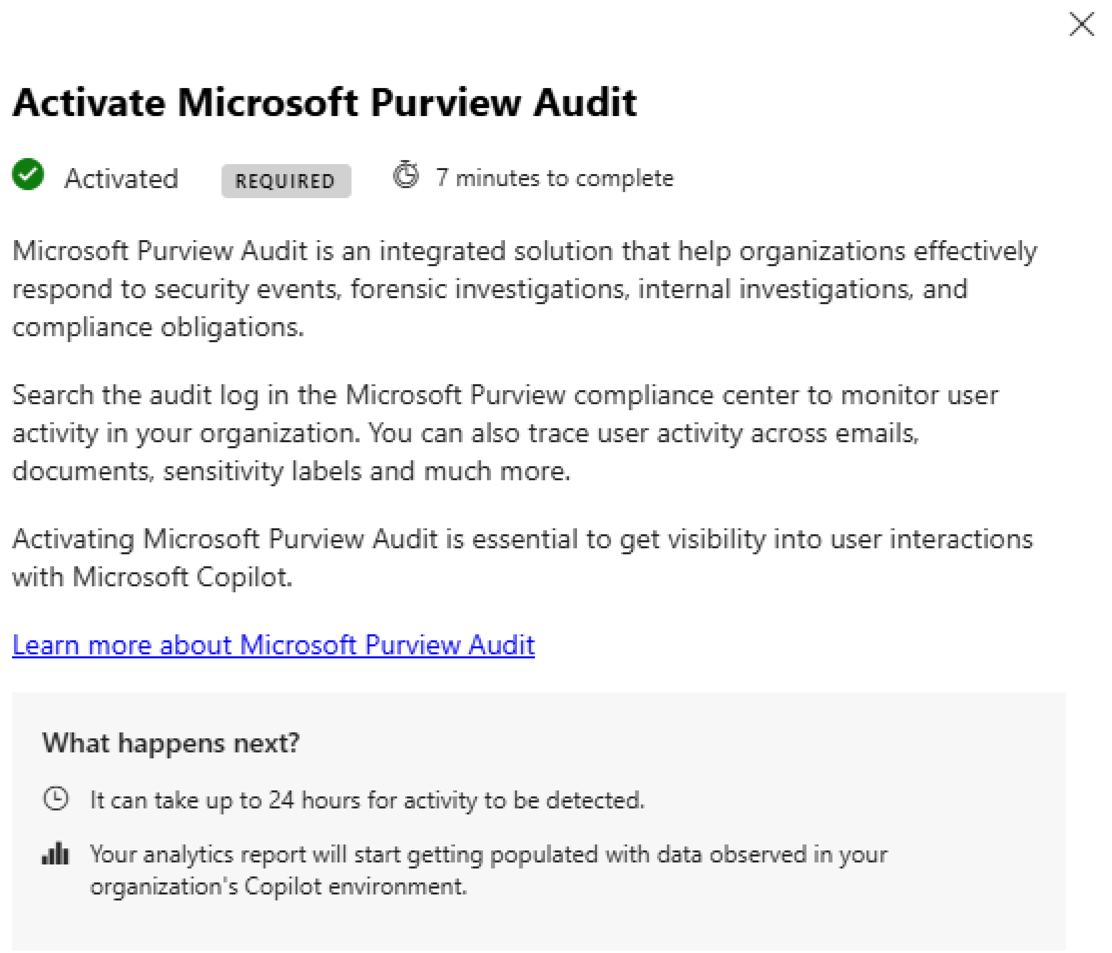
Start Jan 30 00:00

Activities - friendly names

Choose which activities to search for

Activities - operation names

2 Audit shows activated here:



Activate Microsoft Purview Audit

✓ Activated REQUIRED 7 minutes to complete

Microsoft Purview Audit is an integrated solution that help organizations effectively respond to security events, forensic investigations, internal investigations, and compliance obligations.

Search the audit log in the Microsoft Purview compliance center to monitor user activity in your organization. You can also trace user activity across emails, documents, sensitivity labels and much more.

Activating Microsoft Purview Audit is essential to get visibility into user interactions with Microsoft Copilot.

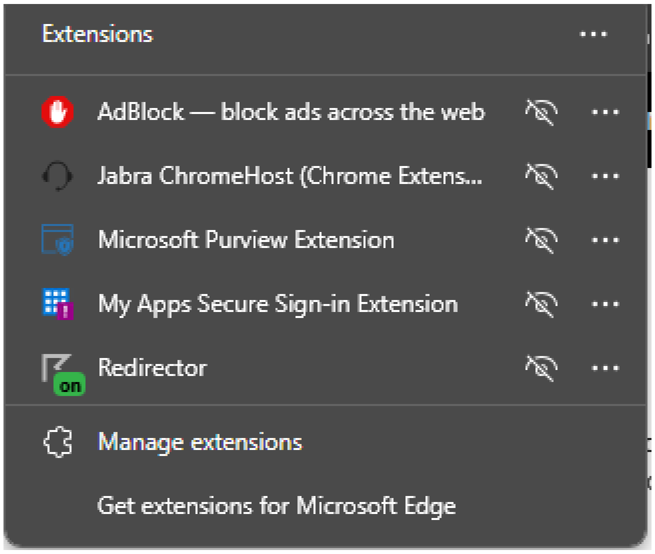
Learn more about Microsoft Purview Audit

What happens next?

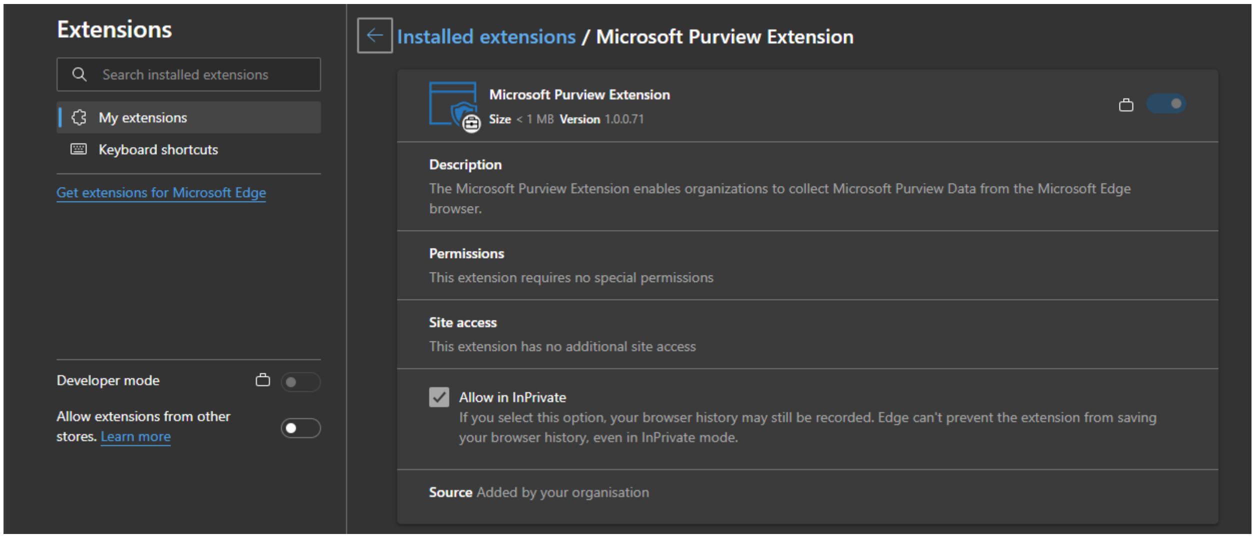
- It can take up to 24 hours for activity to be detected.
- Your analytics report will start getting populated with data observed in your organization's Copilot environment.

Pre-requisite 2: Purview Extension in Browser:

Evidence that Purview Extension is installed in my Edge:


Extensions
AdBlock — block ads across the web
Jabra ChromeHost (Chrome Extens...
Microsoft Purview Extension
My Apps Secure Sign-in Extension
Redirector
on
Manage extensions
Get extensions for Microsoft Edge

Microsoft have also advised that if the extension icon is blue it's enabled. My icon is blue, and displays as enabled in the 'manage extension' screen


Extensions
Search installed extensions
My extensions
Keyboard shortcuts
Get extensions for Microsoft Edge
Developer mode

Allow extensions from other stores. Learn more

Installed extensions / Microsoft Purview Extension

Microsoft Purview Extension

Size < 1 MB **Version** 1.0.0.71

Description

The Microsoft Purview Extension enables organizations to collect Microsoft Purview Data from the Microsoft Edge browser.

Permissions

This extension requires no special permissions

Site access

This extension has no additional site access

☑ Allow in InPrivate

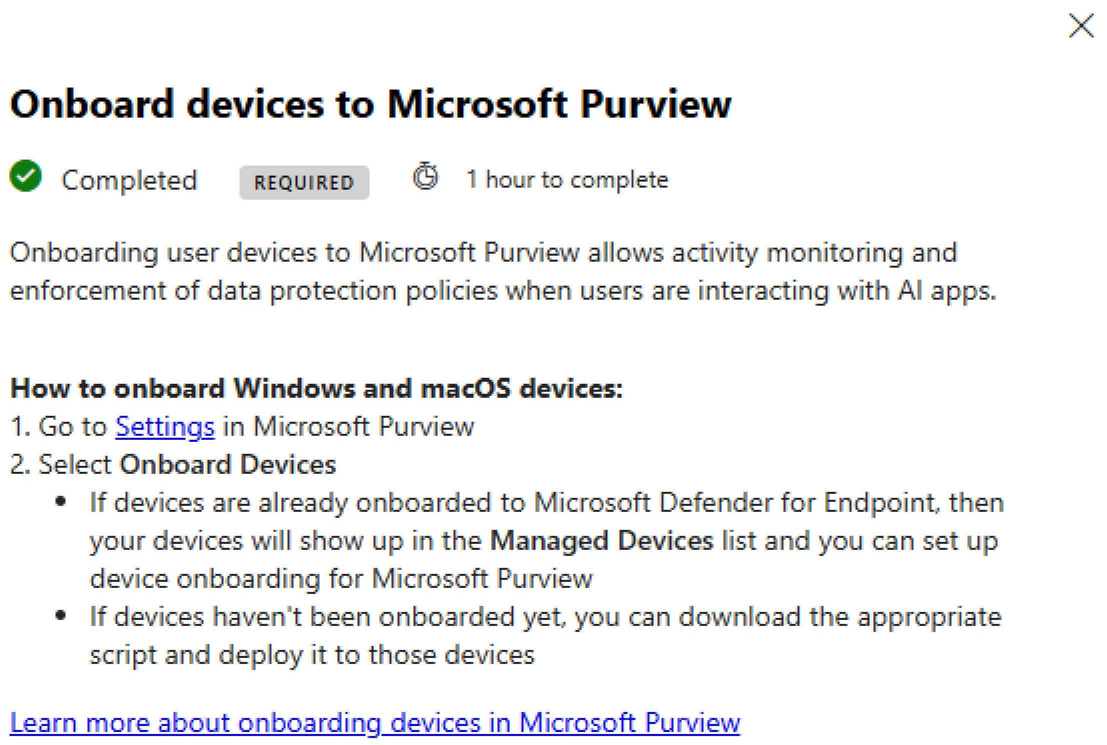
If you select this option, your browser history may still be recorded. Edge can't prevent the extension from saving your browser history, even in InPrivate mode.

Source Added by your organisation

Pre-requisite 3: Device Onboarding:

Evidence that my device is onboarded to Purview:

1: shows completed here:



Onboard devices to Microsoft Purview

✓ Completed REQUIRED 1 hour to complete

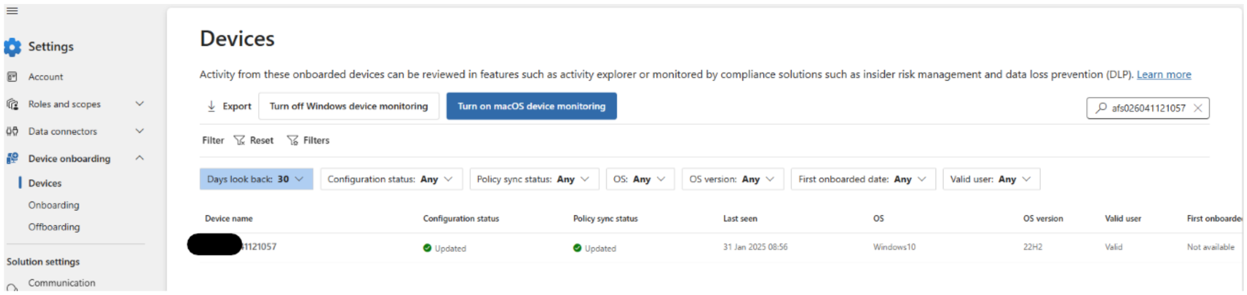
Onboarding user devices to Microsoft Purview allows activity monitoring and enforcement of data protection policies when users are interacting with AI apps.

How to onboard Windows and macOS devices:

1. Go to Settings in Microsoft Purview
2. Select **Onboard Devices**
   - If devices are already onboarded to Microsoft Defender for Endpoint, then your devices will show up in the **Managed Devices** list and you can set up device onboarding for Microsoft Purview
   - If devices haven't been onboarded yet, you can download the appropriate script and deploy it to those devices

Learn more about onboarding devices in Microsoft Purview

2: My device is visible in Purview -> Device Onboarding -> Devices (shown below).



Devices

Activity from these onboarded devices can be reviewed in features such as activity explorer or monitored by compliance solutions such as insider risk management and data loss prevention (DLP). Learn more

afs026041121057

Days look back: **30** Configuration status: **Any** Policy sync status: **Any** OS: **Any** OS version: **Any** First onboarded date: **Any** Valid user: **Any**

Device name	Configuration status	Policy sync status	Last seen	OS	OS version	Valid user	First onboarde
[redacted]1121057	✓ Updated	✓ Updated	31 Jan 2025 08:56	Windows10	22H2	Valid	Not available

Pre-req 4: One click data discovery policies:

Created the suggested one click policies: