

# Workstation – OneDrive Integration

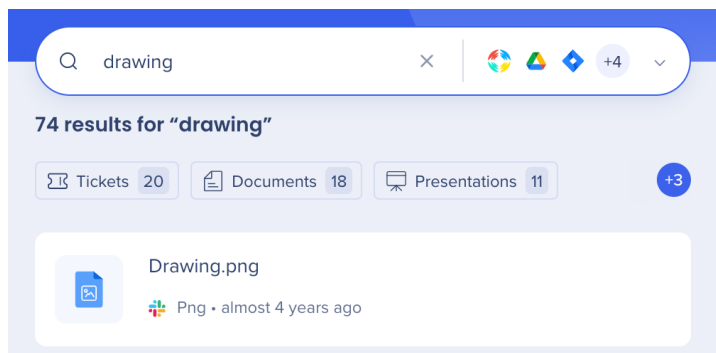
## Brief Overview

Microsoft OneDrive is a file hosting service that Microsoft operates. It enables registered users to share and synchronize their files. OneDrive also works as the storage back-end of the web version of Microsoft Office. OneDrive offers 5 GB of storage space free of charge, with 100 GB, 1 TB, and 6 TB storage options available either separately or with Office 365 subscriptions.

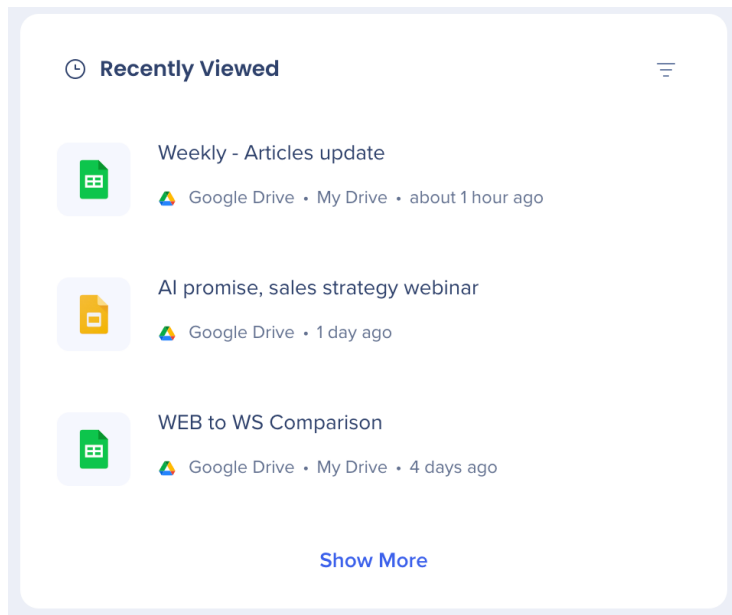
The OneDrive client app adds file synchronization and cloud backup features to its device. The app comes bundled with Microsoft Windows. In addition, Microsoft Office apps directly integrate with OneDrive.

## Use Cases

Search for files stored on OneDrive.

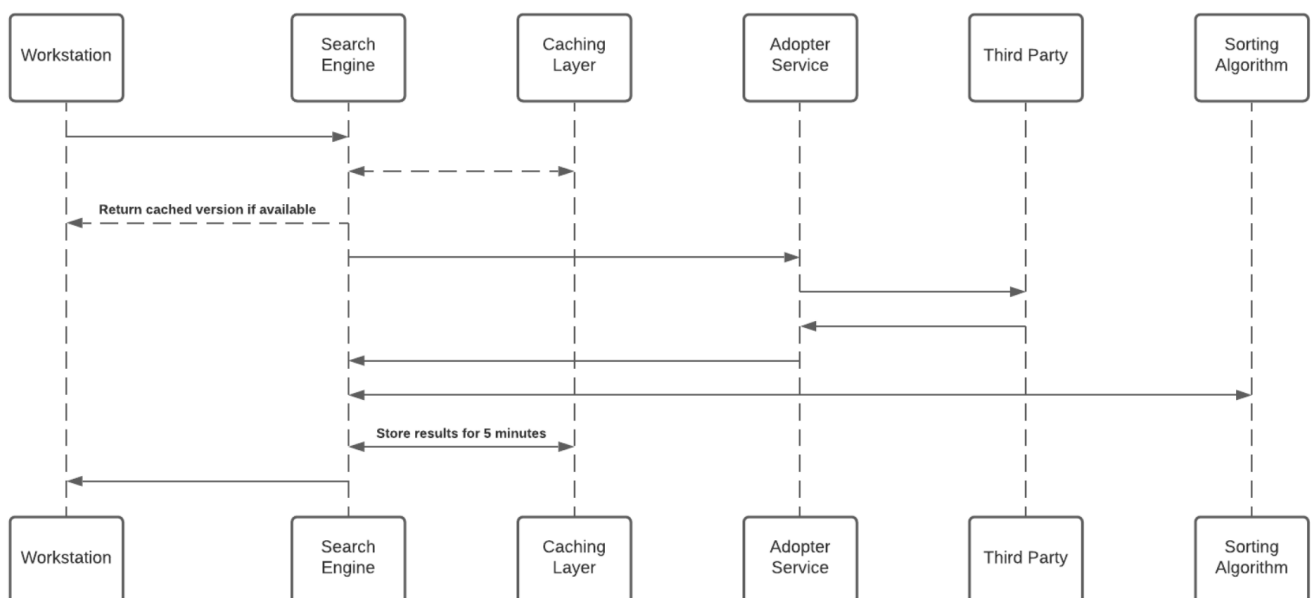


Access recent files from the Recently Viewed widget on the homepage.



## Security

The Enterprise Search uses 3rd-party integrations to implement a “federal search”. Searches within Workstation are backed by an NLP engine, and a graph database that supports a great user experience. Workstation Enterprise Search doesn’t index 3rd-party data on an independently searchable database. See below sequence diagram describes the searching algorithm:



## Notes

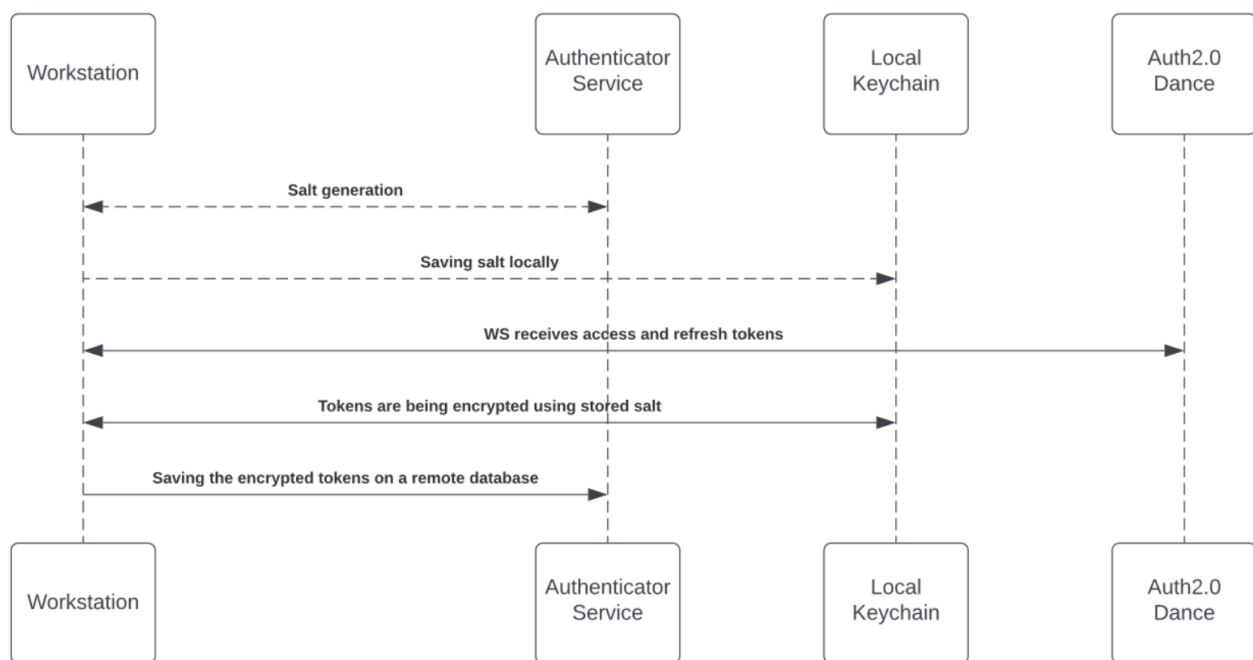
1. Cache layer saves results for a period of five minutes.
2. Each Adopter Service creates a unique identifier for the results which is meaningless without access to the 3rd-party and stores it in the graph database.

### 3rd-Party Access and Refresh Tokens

To activate the Enterprise Search (and the Personalized Workspace widgets), each employee is required to grant Workstation permission to access the 3rd-party. The granting process is using the OAuth2.0 protocol. Each time a new access token is granted to the Workstation, the application will encrypt the access and refresh tokens and store it in a remote database.

The encryption process includes a unique private key ("salt") that is generated for each individual at the very first bootstrap and stored in the local machine Keychain. The salt is irreplaceable and not restorable – **losing it causes the access tokens to be voided**. This security measure is being taken to eliminate identity spoofing when accessing high-sensitive data.

See the diagram below to review the salt generation and storage flow.



## Accessing 3rd-Party Content

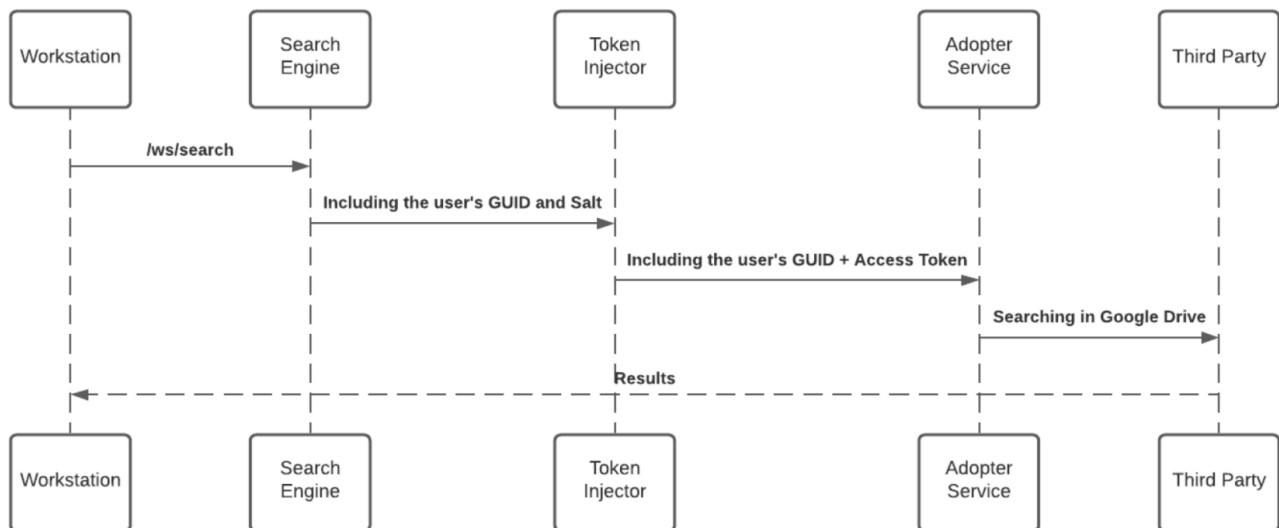
Accessing 3rd-party content requires end-user consent, and in some cases, mostly on Microsoft products, an organization admin consent. End-users grant Workstation the necessary permission by approving an OAuth2.0 consent screen that is being triggered by them from the Workstation

application ("Third-party apps").

The third-party apps are being approved and verified by third-parties products. By the end of the granting process, the third-party apps provide access and refresh tokens that are used by the search engine to establish the requests.

See 3rd-Party Access and Refresh Tokens section above for more information about the storing mechanism.

While searching, the search engine forwards the request, before hitting the Adopter Service, through the Token Injector; a service that injects the relevant tokens to accomplish the request. The local private key is being handed off over the search HTTPS request for runtime decryption.



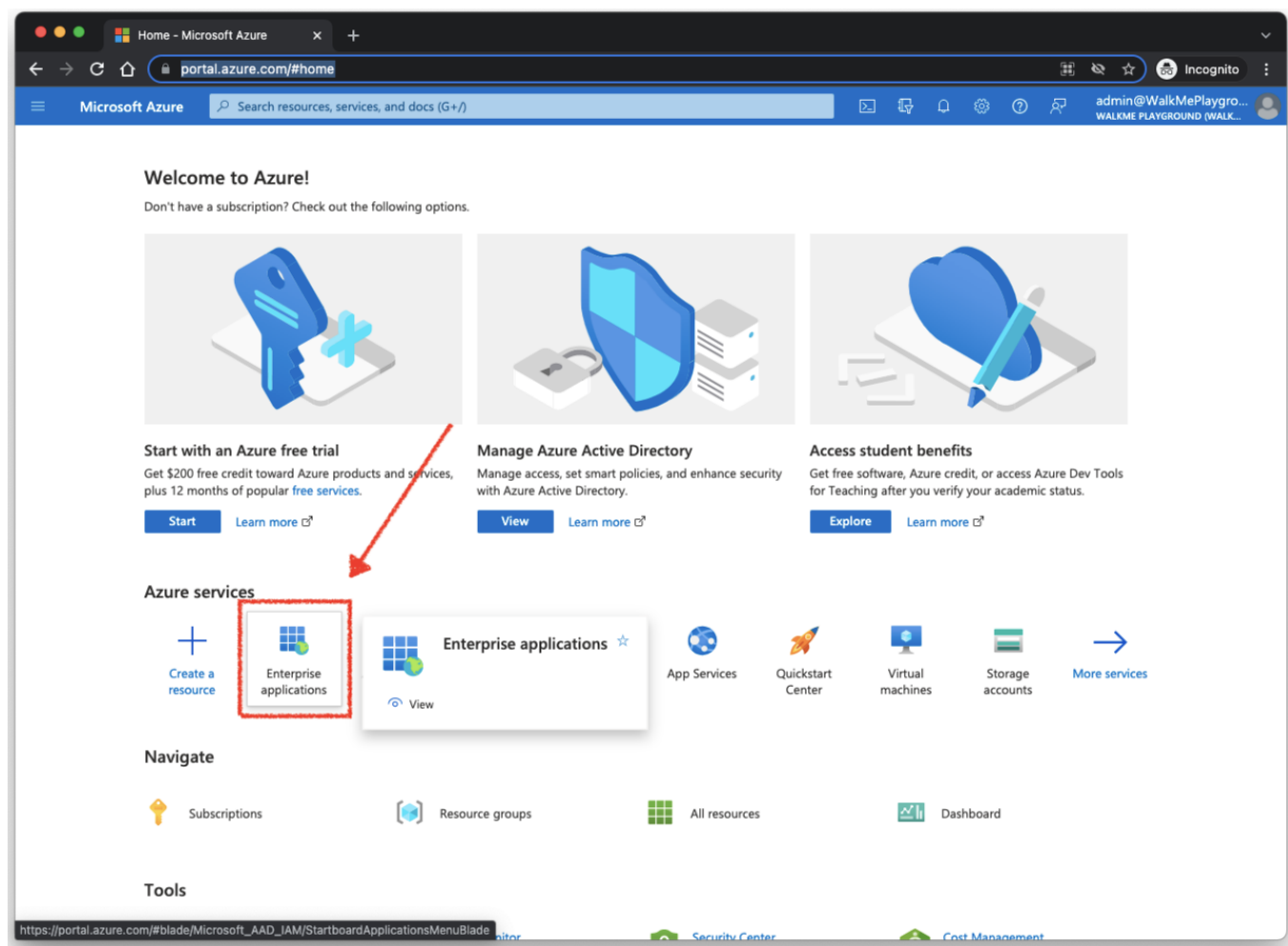
## JWT Protection

When an end-user initiates a search query - the WalkMe enterprise search starts a search flow that is being protected by a JWT assigned by WalkMe IdP integration, as part of the end-user signing flow:

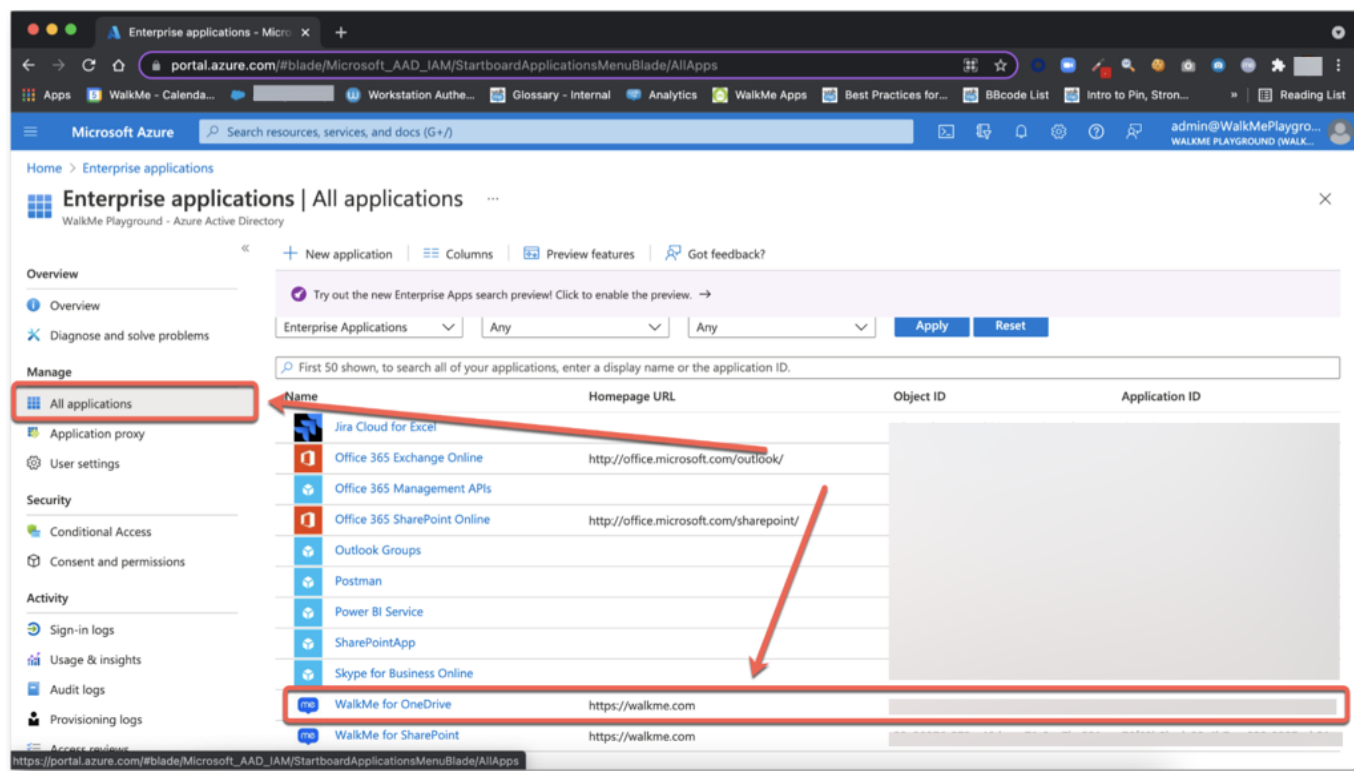


# Grant Administration Consent to WalkMe for OneDrive

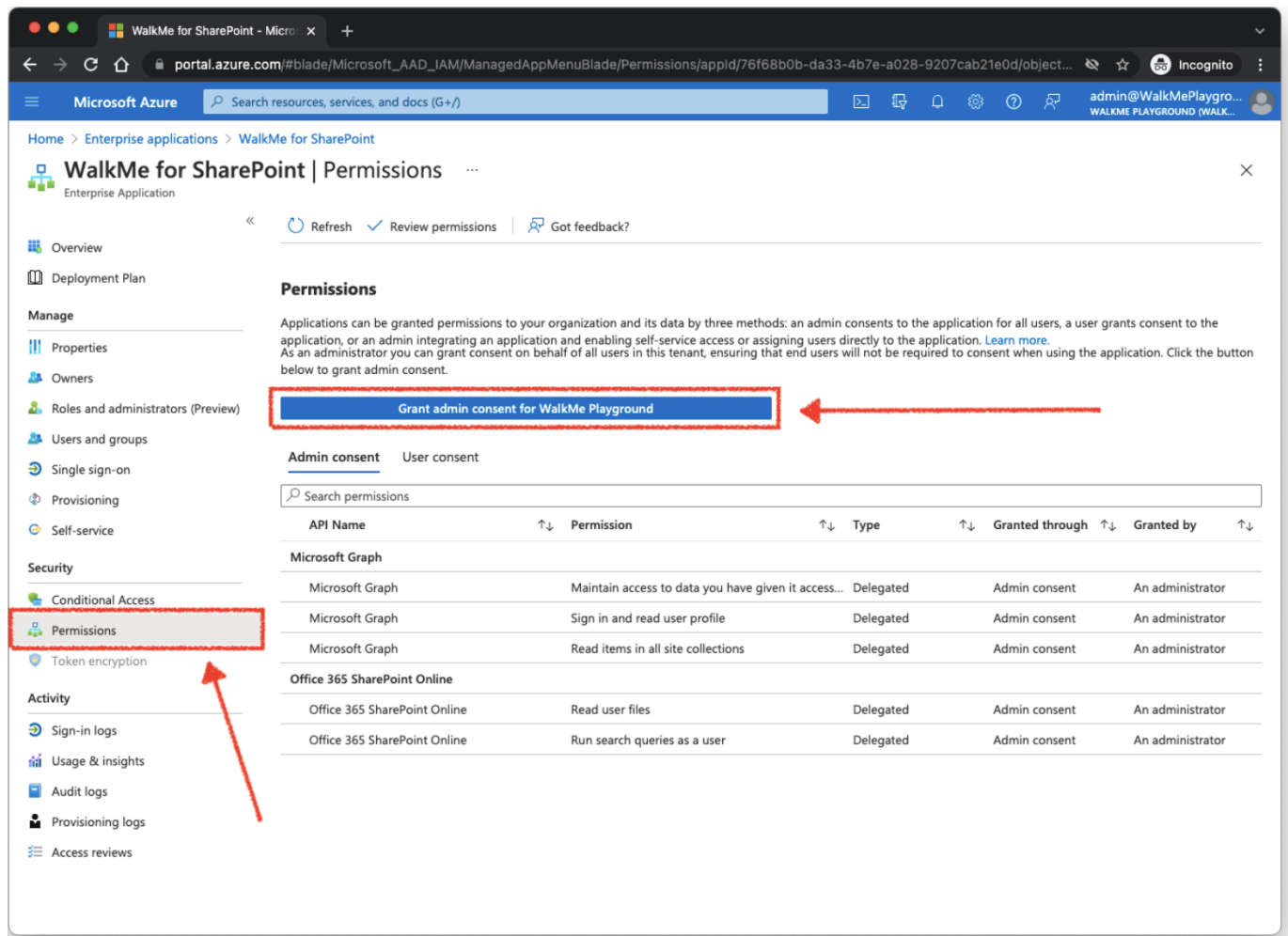
- 71 Stevenson Street, Floor 20 San Francisco, CA 94105 | 245 Fifth Avenue, STE 1501 New York, NY, 10016 | 421 Fayetteville St STE 215 Raleigh, NC 27601 [www.walkme.com](http://www.walkme.com)



#### 4. Select **All Applications** and pick **WalkMe for OneDrive**



5. Select **Permission** tab and click on **Grant admin consent for {{your organization name}}**



Microsoft Azure portal showing the 'WalkMe for SharePoint | Permissions' page. The 'Permissions' tab is selected in the left sidebar. A red box highlights the 'Grant admin consent for WalkMe Playground' button. A red arrow points to this button from the right. Another red arrow points to the 'Permissions' item in the left sidebar.

**Permissions**

Applications can be granted permissions to your organization and its data by three methods: an admin consents to the application for all users, a user grants consent to the application, or an admin integrating an application and enabling self-service access or assigning users directly to the application. [Learn more.](#) As an administrator you can grant consent on behalf of all users in this tenant, ensuring that end users will not be required to consent when using the application. Click the button below to grant admin consent.

**Grant admin consent for WalkMe Playground**

Admin consent | User consent

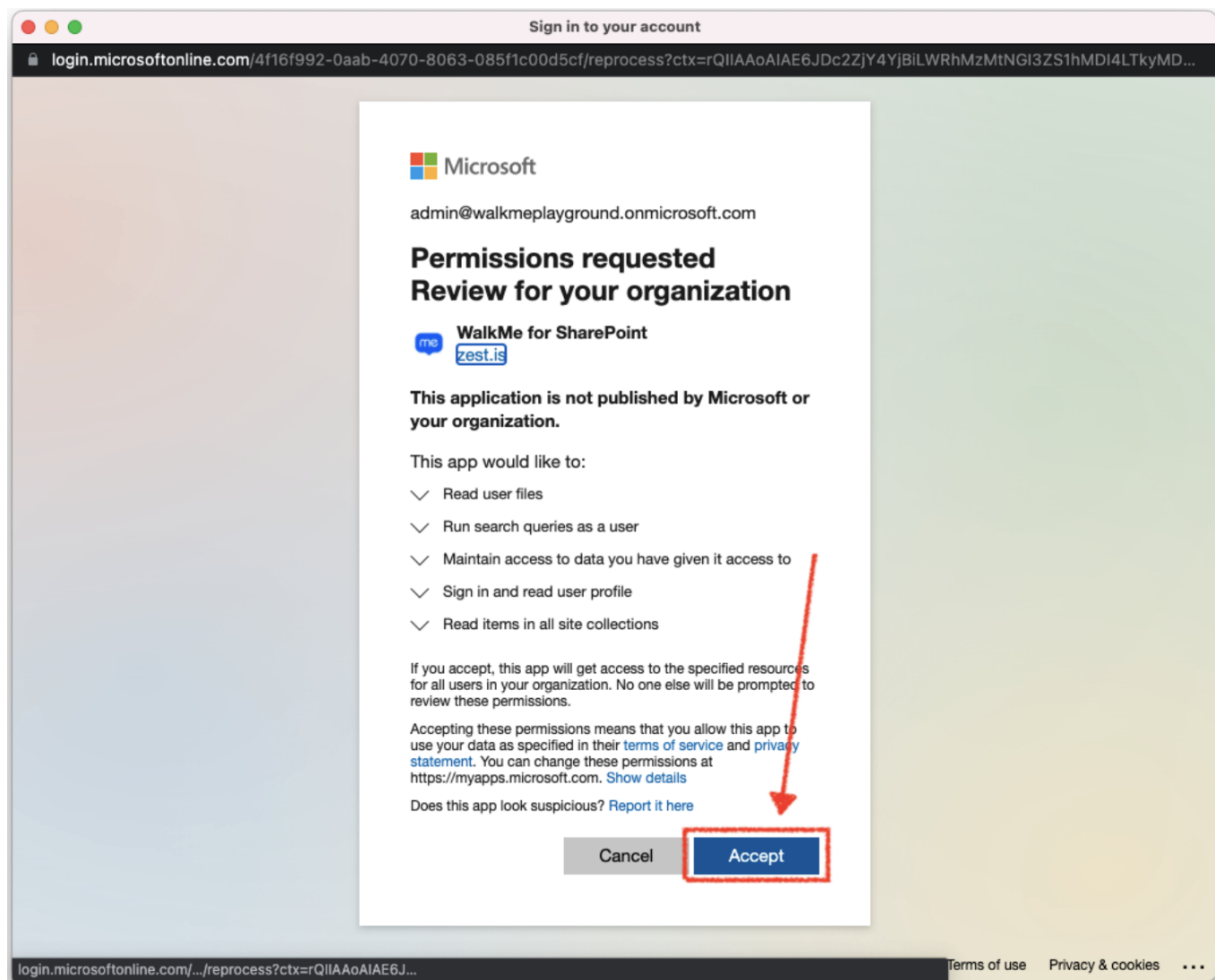
Search permissions

API Name	Permission	Type	Granted through	Granted by
<b>Microsoft Graph</b>				
Microsoft Graph	Maintain access to data you have given it access...	Delegated	Admin consent	An administrator
Microsoft Graph	Sign in and read user profile	Delegated	Admin consent	An administrator
Microsoft Graph	Read items in all site collections	Delegated	Admin consent	An administrator
<b>Office 365 SharePoint Online</b>				
Office 365 SharePoint Online	Read user files	Delegated	Admin consent	An administrator
Office 365 SharePoint Online	Run search queries as a user	Delegated	Admin consent	An administrator

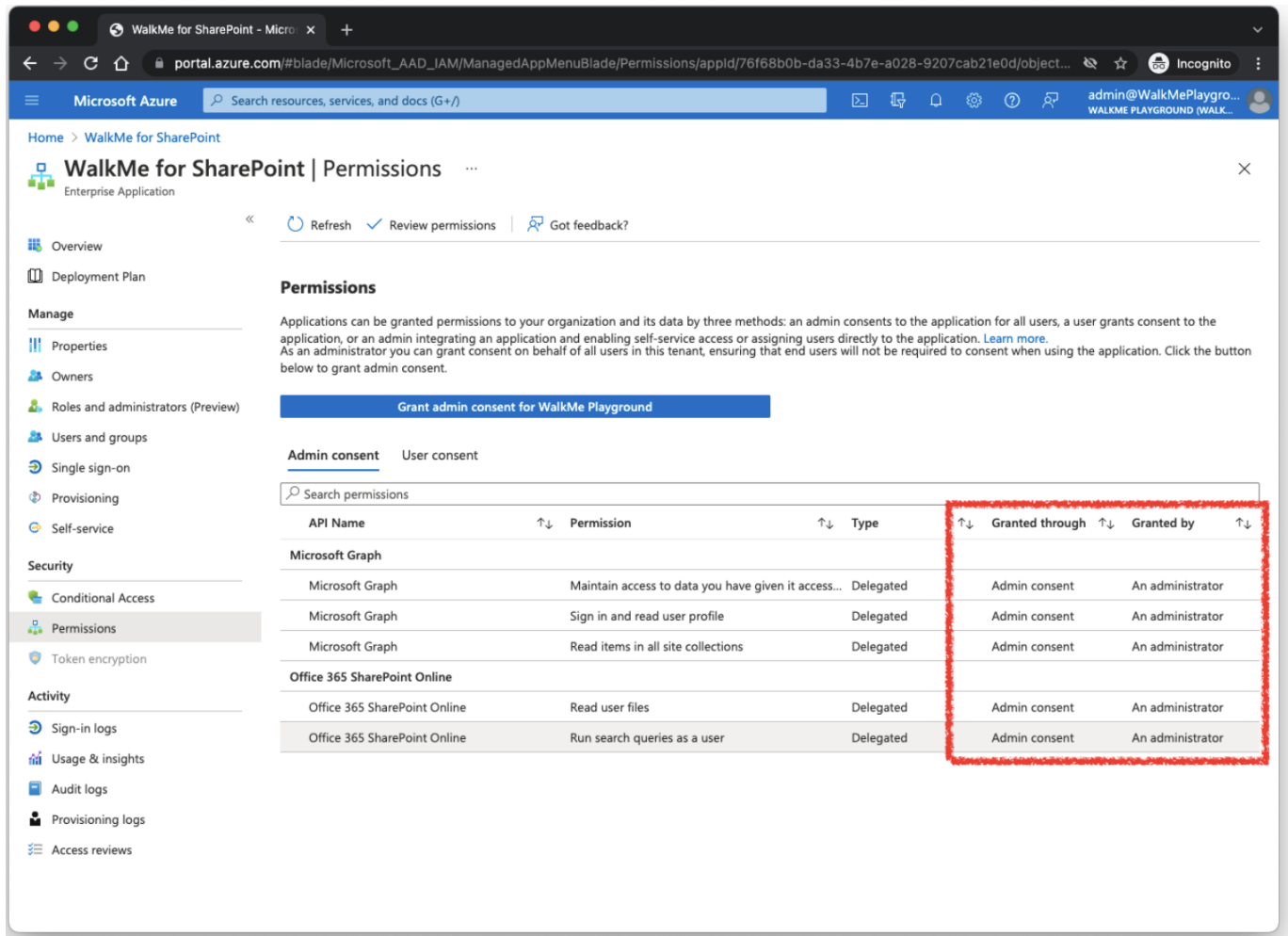
6. Once clicked, a popup should appear (be aware if you have a popup disabler installed) – optionally, you'll be asked to sign in again – **use your Administrator account**

7. Click **Accept** on the dialog, confirming organization users to install, for personal usage, WalkMe for OneDrive





8. Once granted, you shall see a confirmation for each permission on the Application page



Home > WalkMe for SharePoint

## WalkMe for SharePoint | Permissions

Enterprise Application

« Refresh Review permissions Got feedback?

**Permissions**

Applications can be granted permissions to your organization and its data by three methods: an admin consents to the application for all users, a user grants consent to the application, or an admin integrating an application and enabling self-service access or assigning users directly to the application. [Learn more.](#) As an administrator you can grant consent on behalf of all users in this tenant, ensuring that end users will not be required to consent when using the application. Click the button below to grant admin consent.

[Grant admin consent for WalkMe Playground](#)

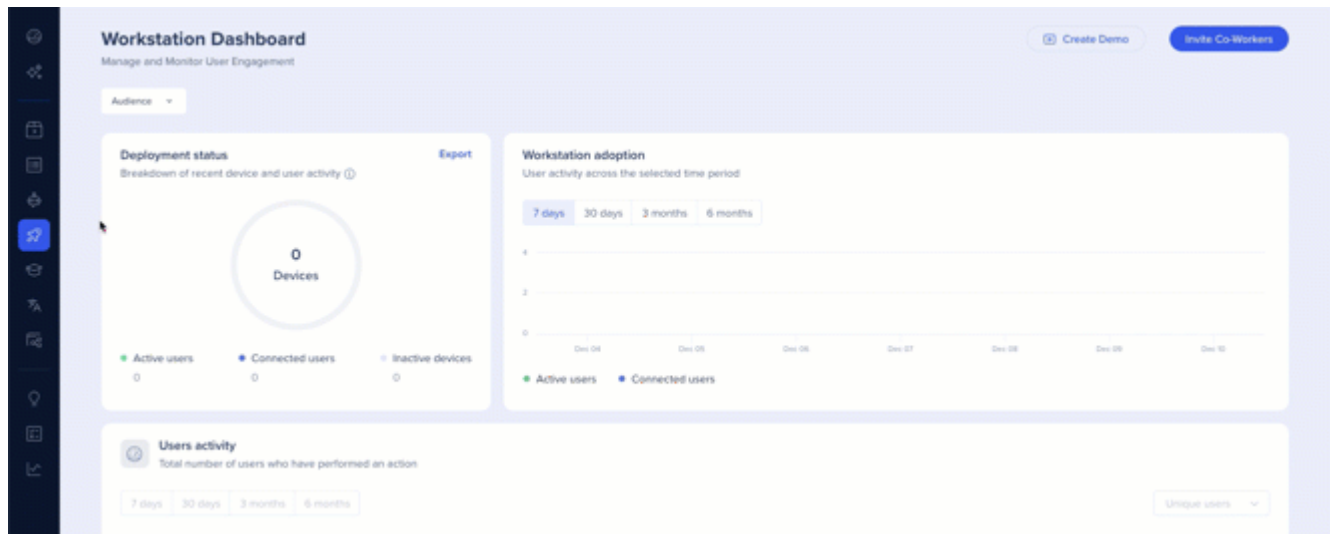
Admin consent User consent

Search permissions

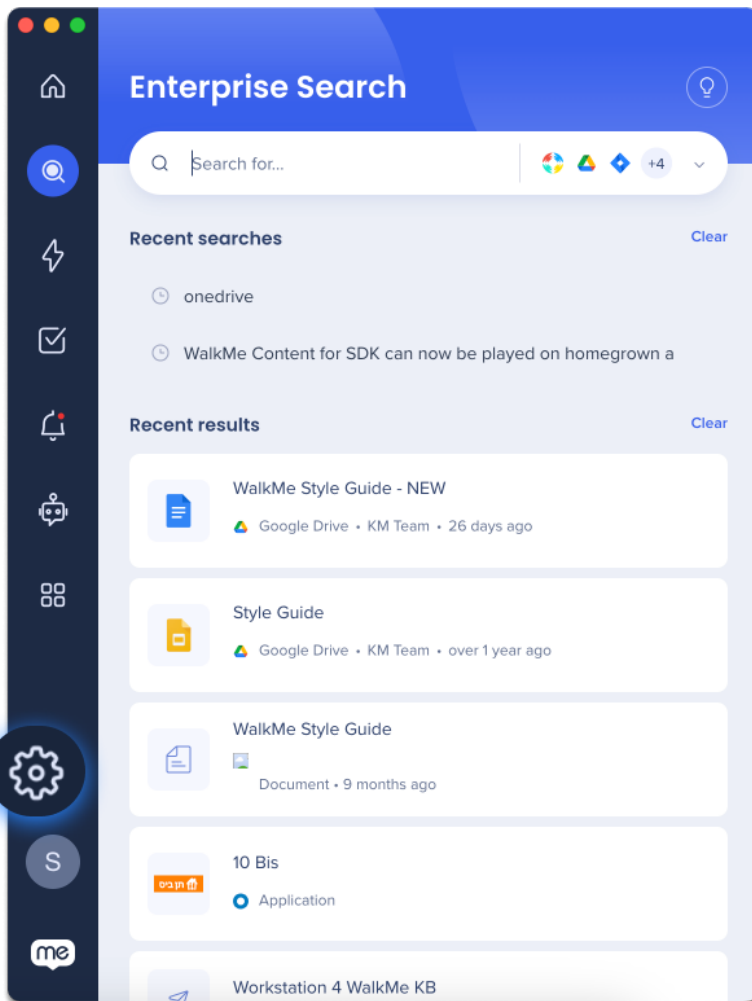
API Name	Permission	Type	Granted through	Granted by
<b>Microsoft Graph</b>				
Microsoft Graph	Maintain access to data you have given it access...	Delegated	Admin consent	An administrator
Microsoft Graph	Sign in and read user profile	Delegated	Admin consent	An administrator
Microsoft Graph	Read items in all site collections	Delegated	Admin consent	An administrator
<b>Office 365 SharePoint Online</b>				
Office 365 SharePoint Online	Read user files	Delegated	Admin consent	An administrator
Office 365 SharePoint Online	Run search queries as a user	Delegated	Admin consent	An administrator

## Installing OneDrive on Workstation

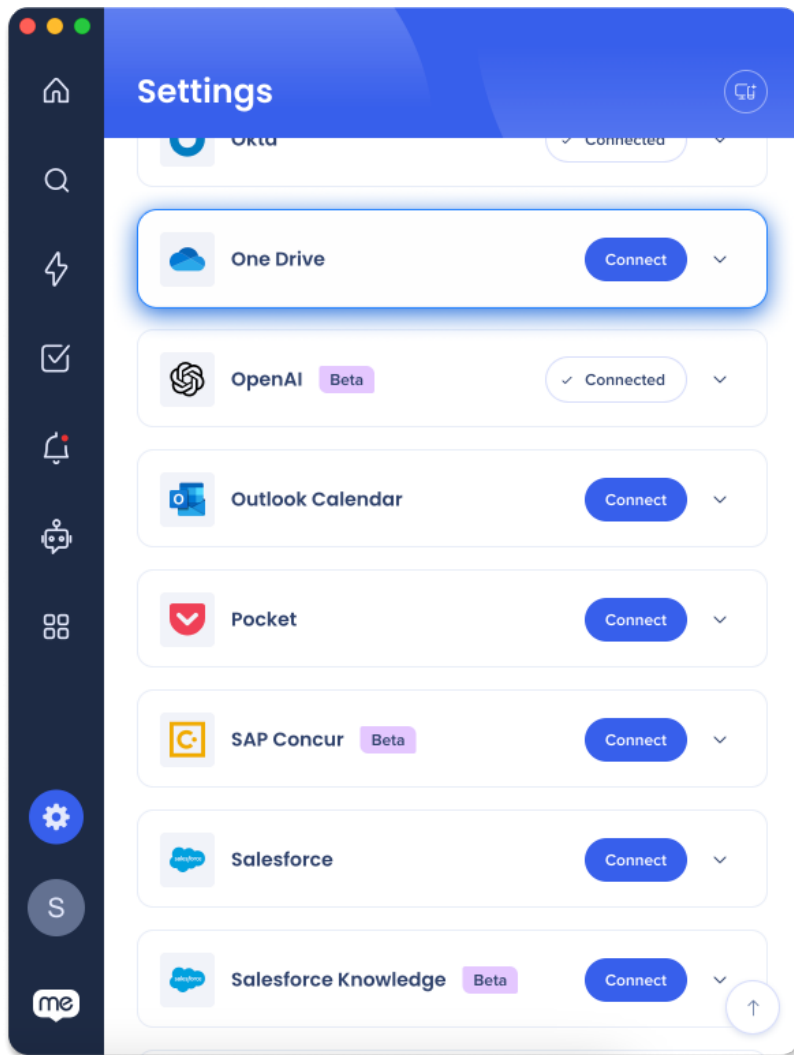
1. Enable the app in [Console](#)



2. Open the Workstation Menu by clicking the widget (on Windows) / the WalkMe icon on the Mac Menu bar, or by hitting ctrl/cmd+shift+E
3. Click the Settings icon in the tabs bar



4. Click **Connect** on the OneDrive card under Integrations



If the OneDrive card is not available, contact your WalkMe Owner in your organization and ask to enable OneDrive on Workstation.

## Segmentation

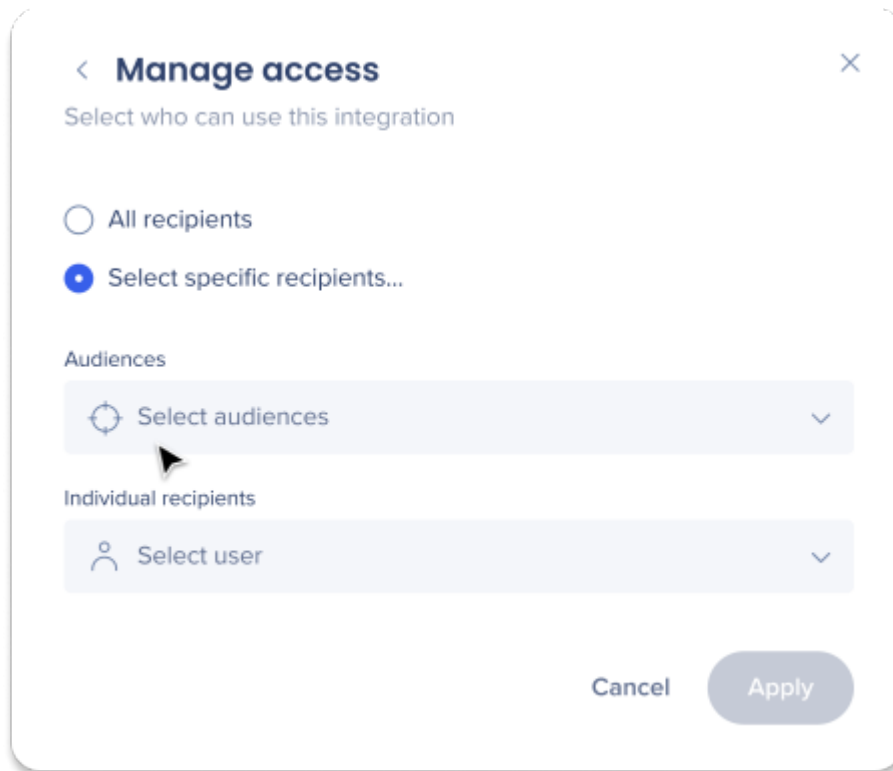
Integrations can be segmented to a sub-set of users and audiences, rather than being enabled for all end-users. This feature streamlines the integration process and helps to ensure that users are only using the integrations that are relevant to their work.

To segment a Workstation integration:

1. Navigate to the [Workstation Integrations page](#) in the console
2. Click the **All button** on the integration you would like to segment
3. Click **Select specific recipients** in the Manage Access popup



4. Select the audiences or individual users from the dropdowns to handpick who can use the integration
5. Click **Apply**



The image shows a 'Manage access' dialog box with a close button (X) in the top right corner. Below the title, it says 'Select who can use this integration'. There are two radio buttons: 'All recipients' (unselected) and 'Select specific recipients...' (selected). Under 'Select specific recipients...', there are two sections: 'Audiences' and 'Individual recipients'. The 'Audiences' section has a dropdown menu with a circular arrow icon and the text 'Select audiences'. The 'Individual recipients' section has a dropdown menu with a person icon and the text 'Select user'. At the bottom right, there are two buttons: 'Cancel' and 'Apply'.

< **Manage access** X

Select who can use this integration

☐ All recipients

☒ Select specific recipients...

Audiences

Select audiences

Individual recipients

Select user

Cancel Apply