

Microsoft Graph API Deep Dive

DevUp 2024

Contact Information:

Matt Henroid

Managing Principal Consultant – Daugherty Business Solutions

<https://www.linkedin.com/in/matthew-henroid/>

Thank you to our Sponsors!



Speaker Introduction

- Professional Developer, Architect and Consultant for 23 years
- 16 years at Daugherty Business Solutions
 - Managing Principal Consultant
 - Enterprise LOS Leader for Software Architecture & Engineering Practice
 - Support an organization of 600 engineers
 - Spend my free time building tools to make my job easier
- Contact me
 - <https://www.linkedin.com/in/matthew-henroid/>
- Code for presentation on Github
 - <https://github.com/mhenroid/devup2024-msgraphapi-demo>



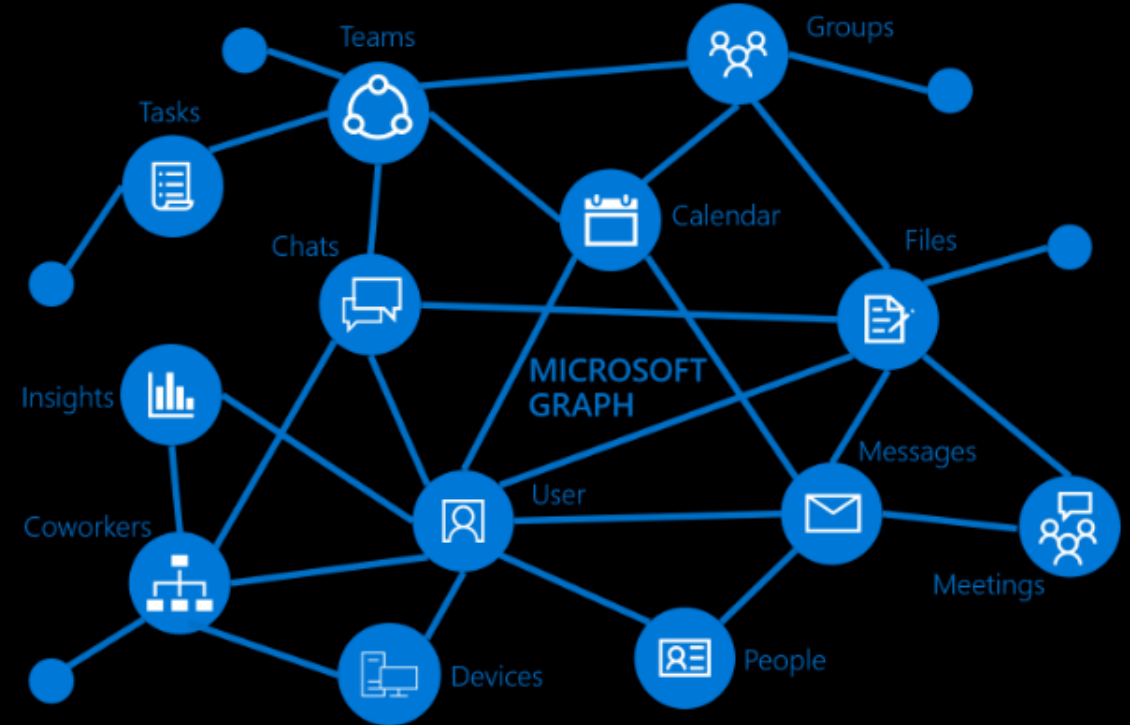
Agenda

- Intro to Microsoft Graph API
- Microsoft Graph API Explorer
- Access Graph using Postman
- Demo App intro
- App Registration
- Run the App



What is Microsoft Graph?

- Gateway to data and intelligence in Microsoft 365
- Services for managing user and device identity, access, compliance and security
- Single endpoint for access to rich people-centric data
- Accessible via REST APIs and language specific SDKs



What can you do with Microsoft Graph?

- View your profile and other people in your organization
- Search your personal and shared OneDrive drives
- Create, Read, Update, Delete files in OneDrive and SharePoint
- Access information in Calendars, Teams, Tasks, Email, OneNote, Groups, etc.
- Automate meeting creation
- Subscribe to changes in calendars or files and send alerts
- View related information for core resources

Graph API Explorer

The easiest way to get started

Microsoft Graph API Explorer

<https://developer.microsoft.com/en-us/graph/graph-explorer>

Microsoft | Microsoft Graph Explore Graph Explorer Docs API Learn Developer Program Support All Microsoft Search

Graph Explorer

Tenant Sample

Sample queries Resources History

Search sample queries

See more queries in the [Microsoft Graph API Reference docs](#).

Getting Started (8)

- GET my profile
- GET my profile (beta)
- GET my photo
- GET my mail
- GET list items in my drive
- GET items trending around me
- GET my manager
- GET my To Do task lists

Applications (8)

Batching (2)

GET v1.0 https://graph.microsoft.com/v1.0/me

Request body Request headers Modify permissions Access token

OK - 200 - 589 ms

Response preview Response headers Code snippets Toolkit component Adaptive cards Expand

You are currently using a sample account. Sign in to access your own data.

```
{
  "@odata.context": "https://graph.microsoft.com/v1.0/$metadata#users/$entity",
  "businessPhones": [
    "+1 412 555 0109"
  ],
  "displayName": "Megan Bowen",
  "givenName": "Megan",
  "jobTitle": "Auditor",
  "mail": "MeganB@M365x214355.onmicrosoft.com",
  "mobilePhone": null,
  "officeLocation": "12/1110",
  "preferredLanguage": "en-US",
  "surname": "Bowen",
  "userPrincipalName": "MeganB@M365x214355.onmicrosoft.com",
  "id": "48d31887-5fad-4d73-a9f5-3c356e68a038"
}
```

* By default, Graph Explorer uses a sample tenant. Use the login button to use your own business tenant

Permissions

- You may not have all the permissions (or scopes) you need to access certain resources
- Use the *Modify permissions* tab to consent
- Some permissions require an account Admin to consent to limit what can be shared

Graph Explorer

Tenant: MSFT

GET v1.0 https://graph.microsoft.com/v1.0/me

Run query

Request body Request headers **Modify permissions** Access token

Permissions

One of the following permissions is required to run the query. If possible, consent to the least privileged permission.

Permission	Description	Admin consent required	Status	Consent type
User.Read	Allows you to sign in to the app with your organizational account and let the app read your profile. It also allows the app to read basic company information.	No	Unconsent	AllPrincipal
Directory.Read.All	Allows the app to read data in your organization's directory.	Yes	Unconsent	AllPrincipal
Directory.ReadWrite.All	Allows the app to read and write data in your organization's directory, such as other users, groups. It does not allow the app to delete users or groups, or reset user passwords.	Yes	Consent	
User.Read.All	Allows the app to read the full set of profile properties, reports, and managers of other users in your organization, on your behalf.	Yes	Consent	
User.ReadBasic.All	Allows the app to read a basic set of profile properties of other users in your organization on your behalf. Includes display name, first and last name, email address and photo.	No	Unconsent	AllPrincipal

OK - 200 - 197 ms

Response preview Response headers Code snippets Toolkit component Adaptive cards Expand

```
{
  "@odata.context": "https://graph.microsoft.com/v1.0/$metadata#users/$entity",
}
```

Top Level Resources

- Use documentation to learn about available resources
<https://learn.microsoft.com/en-us/graph/api/overview?view=graph-rest-1.0>
- Resources have properties and relationships to other resources

URL	Description
https://graph.microsoft.com/v1.0/me	My profile
https://graph.microsoft.com/v1.0/groups	All groups in organization
https://graph.microsoft.com/v1.0/users	All users in organization
https://graph.microsoft.com/v1.0/sites/root	Root SharePoint site for organization
https://graph.microsoft.com/v1.0/applications	Registered applications
https://graph.microsoft.com/v1.0/drives	OneDrive drives the current user has access to

Relationships

- Each resource can have relationships to other resources

URL	Description
https://graph.microsoft.com/v1.0/me/drives	List all my drives
https://graph.microsoft.com/v1.0/me/drive/quota	List the quotas on my default drive
https://graph.microsoft.com/v1.0/groups	List all groups
<a href="https://graph.microsoft.com/v1.0/groups/<groupid>/members">https://graph.microsoft.com/v1.0/groups/<groupid>/members	See all members for a specific group
https://graph.microsoft.com/v1.0/me/drive/root/search(q='My Excel Document')	Search for a particular document by name
<a href="https://graph.microsoft.com/v1.0/me/drives/<driveid>/items/root/children">https://graph.microsoft.com/v1.0/me/drives/<driveid>/items/root/children	See all files in a specific drive

Query Parameters

- Use Query Parameters to filter, sort, search resources, select properties, and expand children
- <https://learn.microsoft.com/en-us/graph/query-parameters>

Name	Description	Example
\$count	Retrieves the total count of matching resources.	/me/messages? \$top=2&\$count=true
\$expand	Retrieves related resources.	/groups?\$expand=members
\$filter	Filters results (rows).	/users? \$filter=startswith(givenName,'J')
\$format	Returns the results in the specified media format.	/users?\$format=json
\$orderby	Orders results.	/users?\$orderby=displayName desc
\$search	Returns results based on search criteria.	/me/messages?\$search=pizza
\$select	Filters properties (columns).	/users?\$select=givenName,surname
\$skip	Indexes into a result set. Also used by some APIs to implement paging and can be used together with <code>\$top</code> to manually page results.	/me/messages?\$skip=11
\$top	Sets the page size of results.	/users?\$top=2

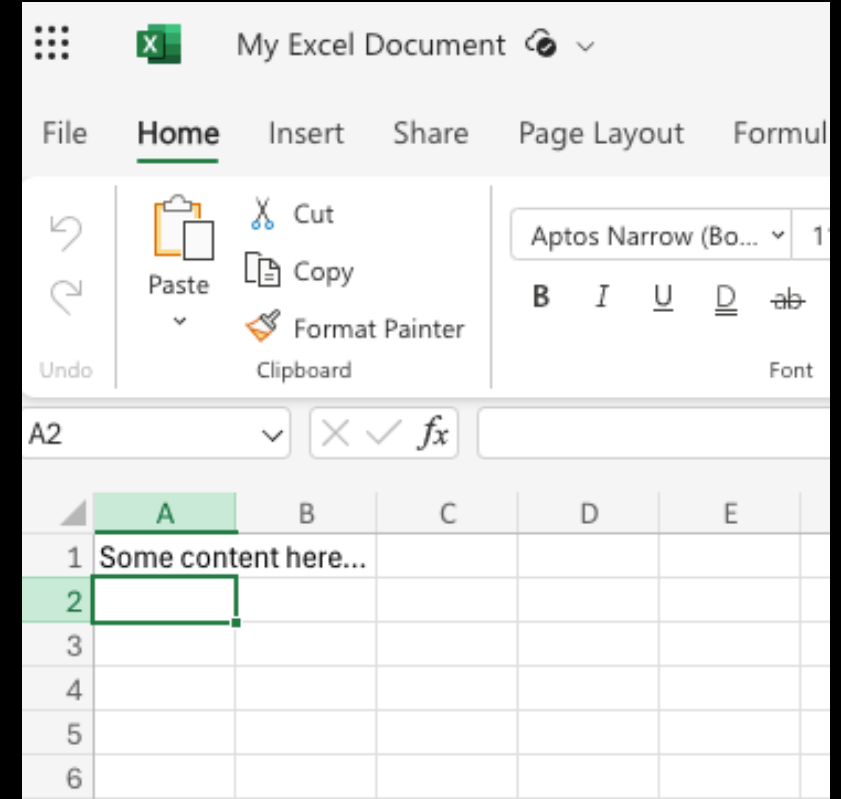
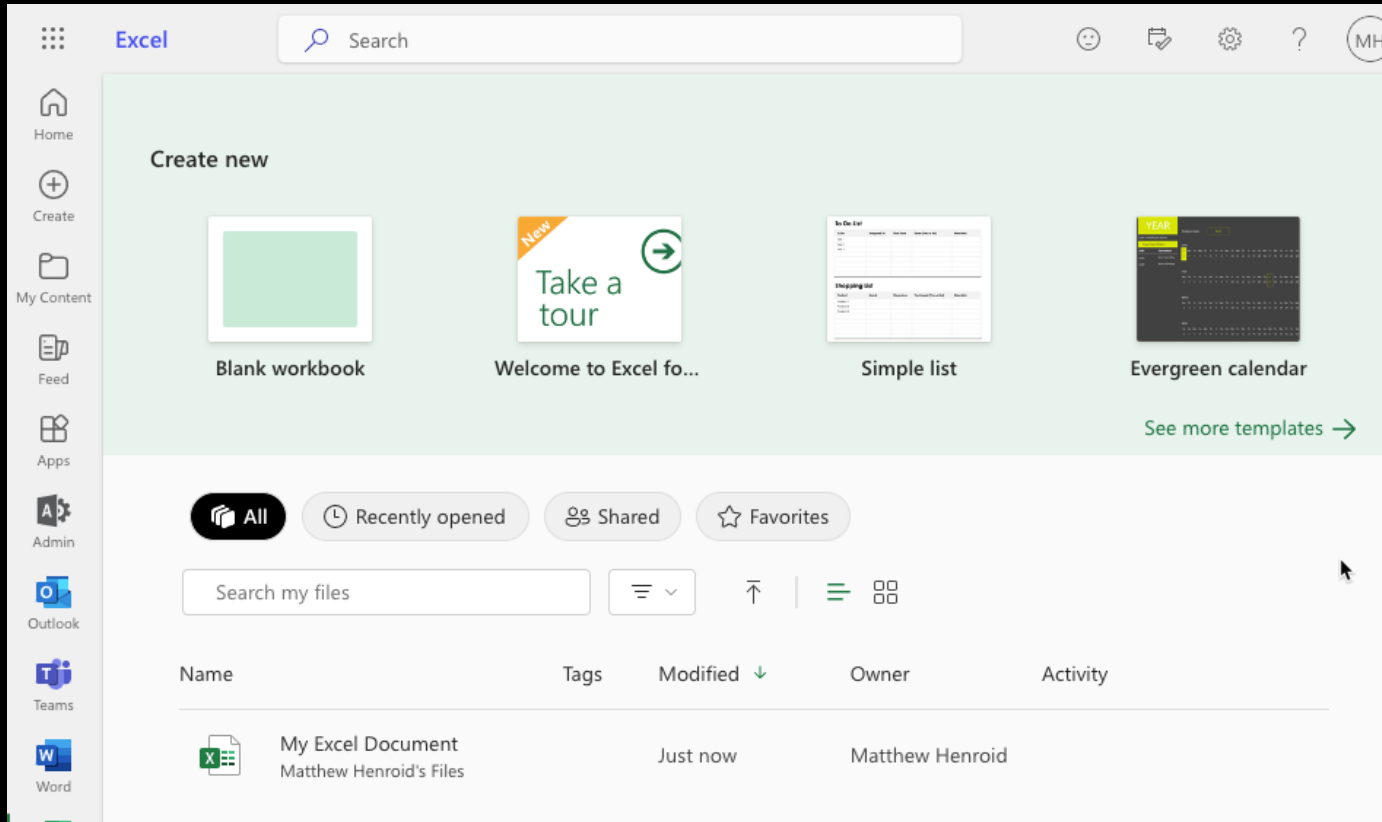
Query Parameters

URL	Description
<code>https://graph.microsoft.com/v1.0/users?\$select=id,displayName,mail</code>	Display only specific fields
<code>https://graph.microsoft.com/v1.0/users?\$search="displayName:Matthew"</code> Requires request header "ConsistencyLevel: eventual"	Search users by displayName
<code>https://graph.microsoft.com/v1.0/users?\$filter=startsWith(givenName, 'M')</code>	Filter users where givenName starts with 'M'
<code>https://graph.microsoft.com/v1.0/users?\$top=2</code>	Display only the top 2 users (see skip token)
<code>https://graph.microsoft.com/v1.0/users?\$top=2&\$skiptoken=<skipToken></code>	Go to the next page to display 2 more users
<code>https://graph.microsoft.com/v1.0/groups?\$expand=members</code>	Display all groups and also members for those groups
<code>https://graph.microsoft.com/v1.0/groups?\$select=id,displayName,description&\$expand=members(\$select=id,displayName)</code>	Display all groups and members but only display certain fields

- By default search results don't always display all properties. Use documentation + \$select to display the fields you need
- You're encouraged to use \$select to limit search results which improves performance

Accessing files

- Let's create an Excel document



Accessing files

Let's view recently accessed files

<https://graph.microsoft.com/v1.0/me/drive/recent>

The screenshot shows the Microsoft Graph Explorer interface. The top navigation bar includes the Microsoft logo, 'Microsoft Graph', and various links like 'Explore', 'Graph Explorer', 'Docs', 'API', 'Learn', 'Developer Program', and 'Support'. The right side of the top bar shows 'All Microsoft' and a search icon. The main header area includes 'Graph Explorer', 'Tenant MSFT', a settings gear, a help icon, and a user profile icon labeled 'MH'.

The left sidebar contains 'Sample queries', 'Resources', and 'History'. Under 'Sample queries', there is a search bar and a list of queries: 'Microsoft Teams (beta) (7)', 'Microsoft To Do (4)', 'Notifications (beta) (2)', and 'OneDrive (5)'. The 'OneDrive (5)' section is expanded, showing a list of queries: 'GET list items in my drive', 'GET my recent files', 'GET files shared with me', 'GET search my OneDrive', and 'POST create a folder'.

The main content area shows the 'Modify permissions' tab for the query 'https://graph.microsoft.com/v1.0/me/drive/recent'. The message states: 'No resource was found matching this query'. Below this, there are tabs for 'Request body', 'Request headers', 'Modify permissions', and 'Access token'. The 'Modify permissions' tab is active, displaying a table of permissions required to run the query.

Permission	Description	Consent Status	Action
Files.Read	Allows the app to read your files.	No	Consent
Files.Read.All	Allows the app to read all files you can access.	No	Consent
Files.ReadWrite	Allows the app to read, create, update, and delete your files.	No	Consent
Files.ReadWrite.All	Allows the app to read, create, update and delete all files that you can access.	No	Consent
Sites.Read.All	Allow the application to read documents and list items in all site collections on your behalf	No	Unconsent
Sites.ReadWrite.All	Allow the application to edit or delete documents and list items in all site collections on your behalf.	No	Consent

A tooltip 'Modify permissions' is visible over the 'Unconsent' button for 'Sites.Read.All'. At the bottom, a status bar shows 'OK - 200 - 822 ms'.

Accessing files

Graph Explorer

Tenant MSFT

MH

Sample queries

Resources

History

Search sample queries

See more queries in the [Microsoft Graph API Reference docs](#).

> Microsoft Teams (beta) (7)

> Microsoft To Do (4)

> Notifications (beta) (2)

> OneDrive (5)

> OneNote (6)

> Outlook Calendar (7)

> Outlook Mail (10)

> Outlook Mail (beta) (1)

GET v1.0 https://graph.microsoft.com/v1.0/me/drive/recent

No resource was found matching this query

Request body

Request headers

Modify permissions

Access token

OK - 200 - 600 ms

Response preview

Response headers

Code snippets

Toolkit component

Adaptive cards

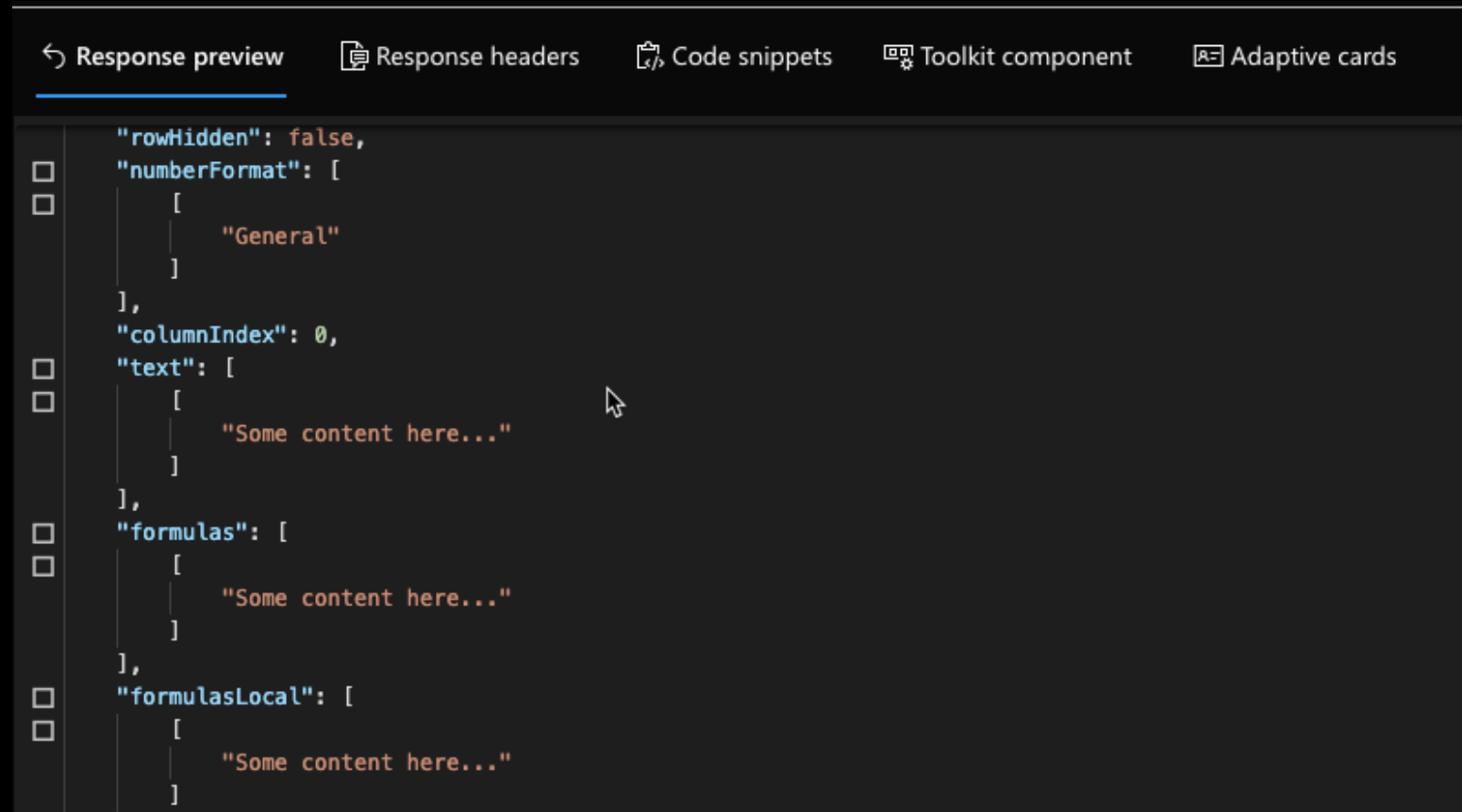
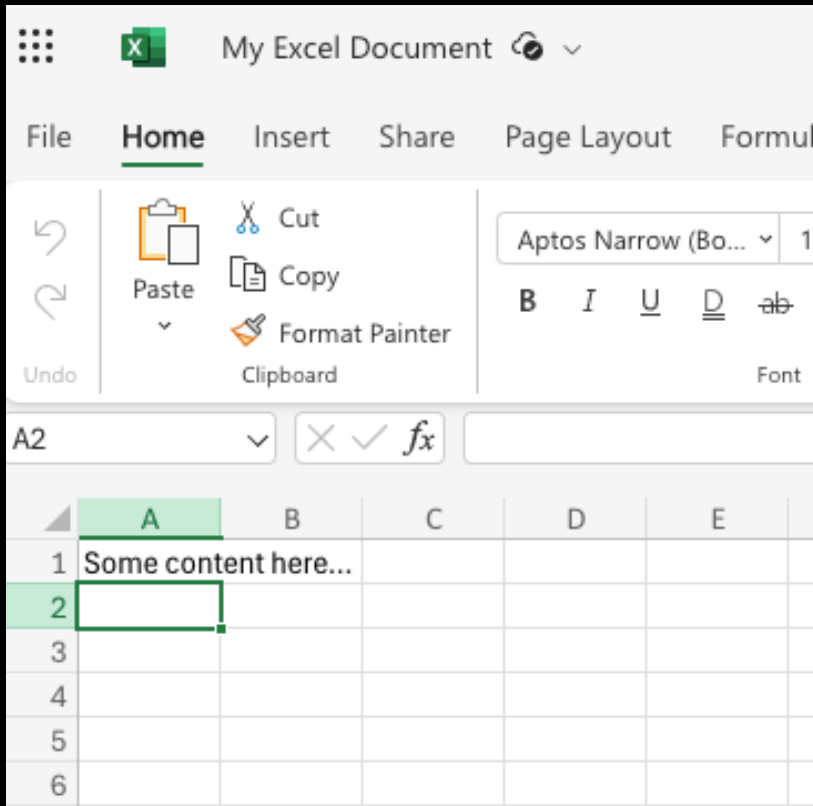
Expand

```
{
  "@odata.context": "https://graph.microsoft.com/v1.0/$metadata#Collection(microsoft.graph.driveItem)",
  "@microsoft.graph.tips": "Use $select to choose only the properties your app needs, as this can lead to performance improvements. For example: GET me/drive/microsoft.graph.recent?$select=audio,bundle",
  "value": [
    {
      "createdDateTime": "2024-08-11T17:18:57Z",
      "id": "01FSSII2HXBI7XWNIYTZCKHN6MID6L2NLW",
      "lastModifiedDateTime": "2024-08-11T17:18:59Z",
      "name": "My Excel Document.xlsx",
      "size": 6339,
      "webUrl": "https://47bjpv-my.sharepoint.com/personal/admin_47bjpv_onmicrosoft_com/_layouts/15/Doc.aspx?sourcedoc=%7B7B3F0AF7-1835-449E-A3B7-CC40FCBD3576%7D&file=Book.xlsx&action=default&mobileredirect=true",
      "createdBy": {
        "user": {
          "displayName": "Matthew Henroid",
          "email": "admin@47bjpv.onmicrosoft.com"
        }
      },
      "lastModifiedBy": {
        "user": {
          "displayName": "Matthew Henroid",
          "email": "admin@47bjpv.onmicrosoft.com"
        }
      }
    }
  ]
}
```


Accessing files

What about viewing contents of an Excel document?

[https://graph.microsoft.com/v1.0/me/drive/items/01FSSII2HXBI7XWNIYTZCKHN6MID6L2NLW/workbook/worksheets/Sheet1/range/cell\(row=0,column=0\)](https://graph.microsoft.com/v1.0/me/drive/items/01FSSII2HXBI7XWNIYTZCKHN6MID6L2NLW/workbook/worksheets/Sheet1/range/cell(row=0,column=0))



Postman

Using Postman or other API tools

Using Postman

Can we do the same with Postman?

Looks like there's an error because of a missing Access Token

The screenshot shows the Postman interface with a GET request to `https://graph.microsoft.com/v1.0/me/drive/items/01FSSII2HXB7XWNIYTZCKHN6MID6L2NLW/workbook/worksheets/Sheet1/range/...`. The request is saved and has 7 headers. The response is a 401 Unauthorized error with the message "Access token is empty." and a request ID.

Query Params

Key	Value	Description	...	Bulk Edit
Key	Value	Description		

Body Cookies Headers (11) Test Results

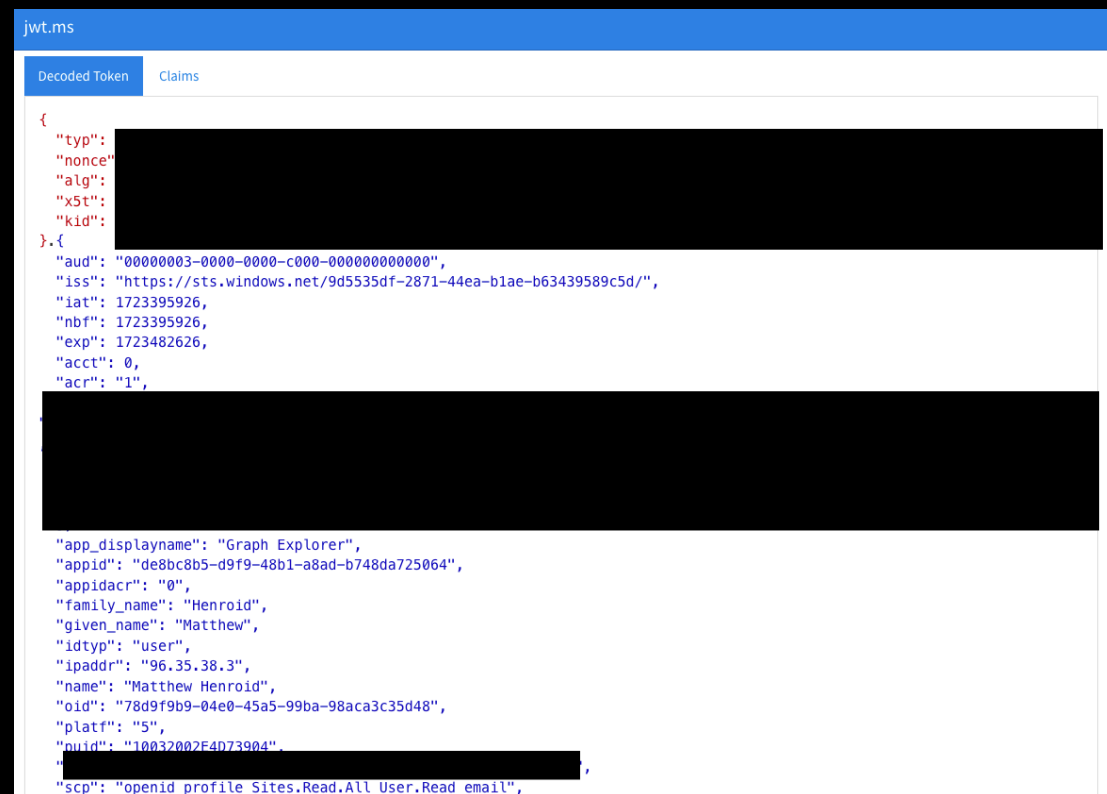
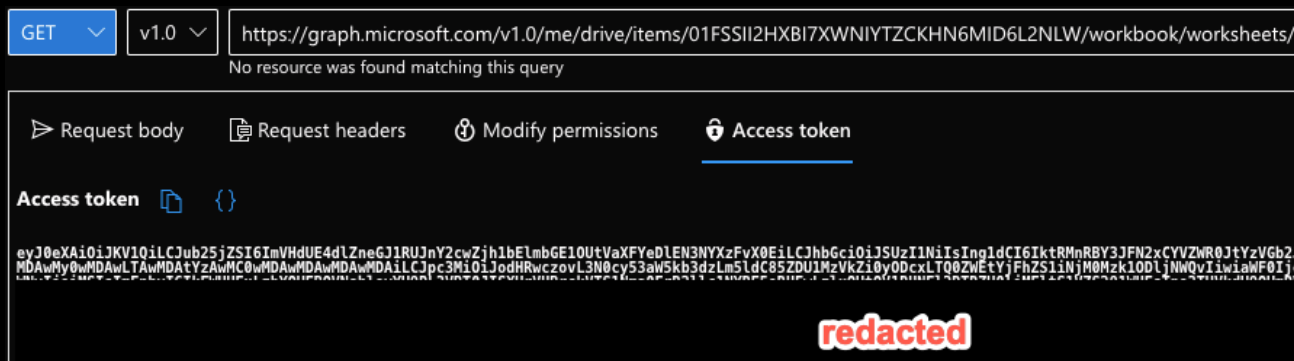
Status: 401 Unauthorized Time: 193 ms Size: 1.48 KB Save as example

Pretty Raw Preview Visualize JSON

```
1 {"error":{"code":"InvalidAuthenticationToken","message":"Access token is empty.","innerError":{"date":"2024-08-11T17:45:10","request-id":"aafa30f9-5c4d-44ee-93e2-0a4853acc2e5","client-request-id":"aafa30f9-5c4d-44ee-93e2-0a4853acc2e5"}}}
```

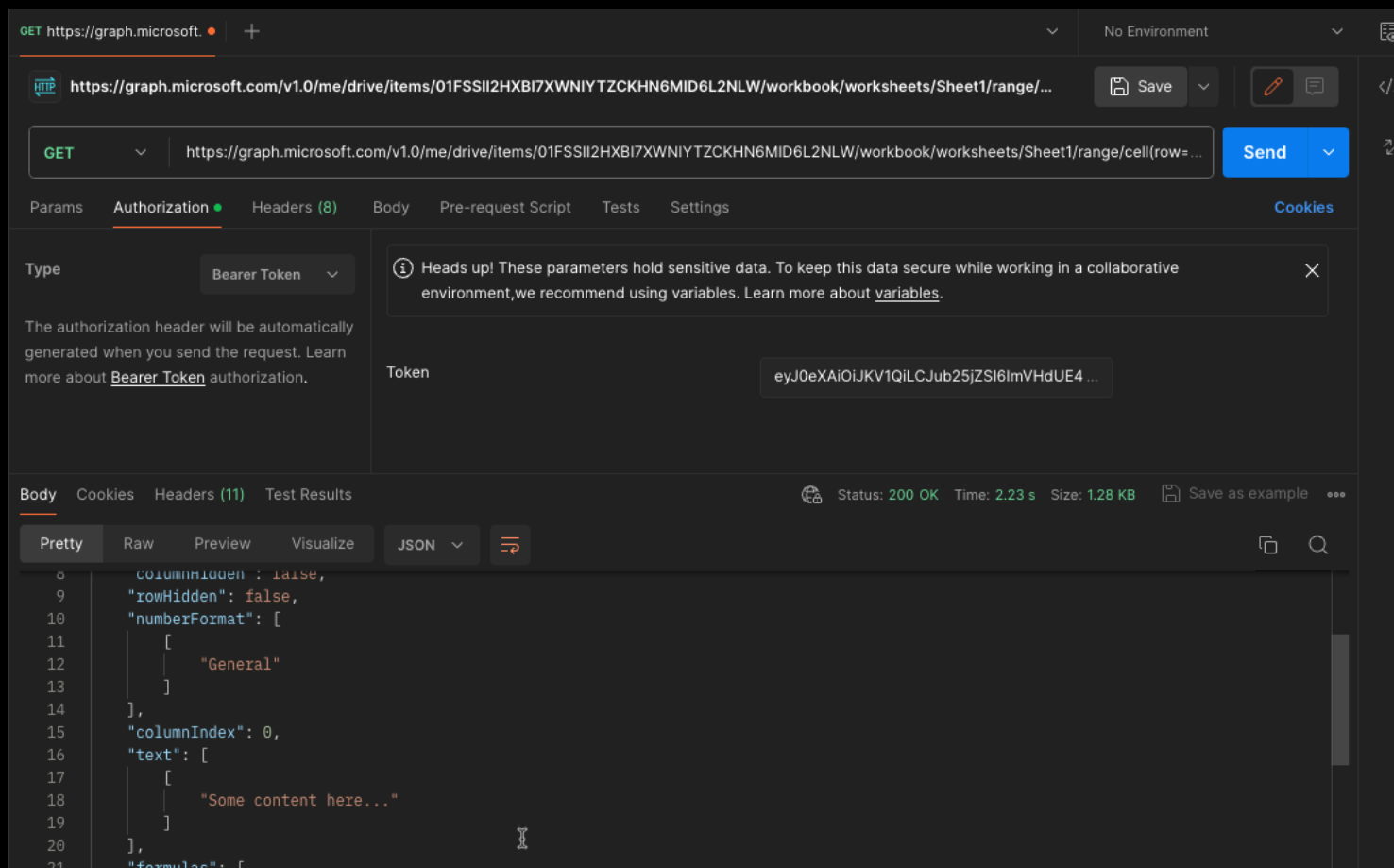
Access Tokens

- Use the *Access token* tool in Graph Explorer to get a temporary access token
- Never, ever, ever share an access token with anyone (you might as well give them your password)
- Tokens expire after 20-28 hours
- Use jwt.ms to decode a JWT (which is created by Microsoft; don't use any other or risk getting hacked)



Setting Bearer token

- Use the Authorization tab and set the Bearer token
- Now everything works (for at least the next day)



Access Tokens

- Remember, our Access Token is short lived
- It's also tied directly to a specific application
- It is also tightly coupled to the available permission / scopes allowed / requested

```
"aud": "00000003-0000-0000-c000-000000000000",  
"iss": "https://sts.windows.net/9d5535df-2871-44ea-b1ae-b63439589c5d/",  
"iat": 1723395926,  
"nbf": 1723395926,  
"exp": 1723482626,  
"acct": 0,  
"acr": "1",  
"aio":
```

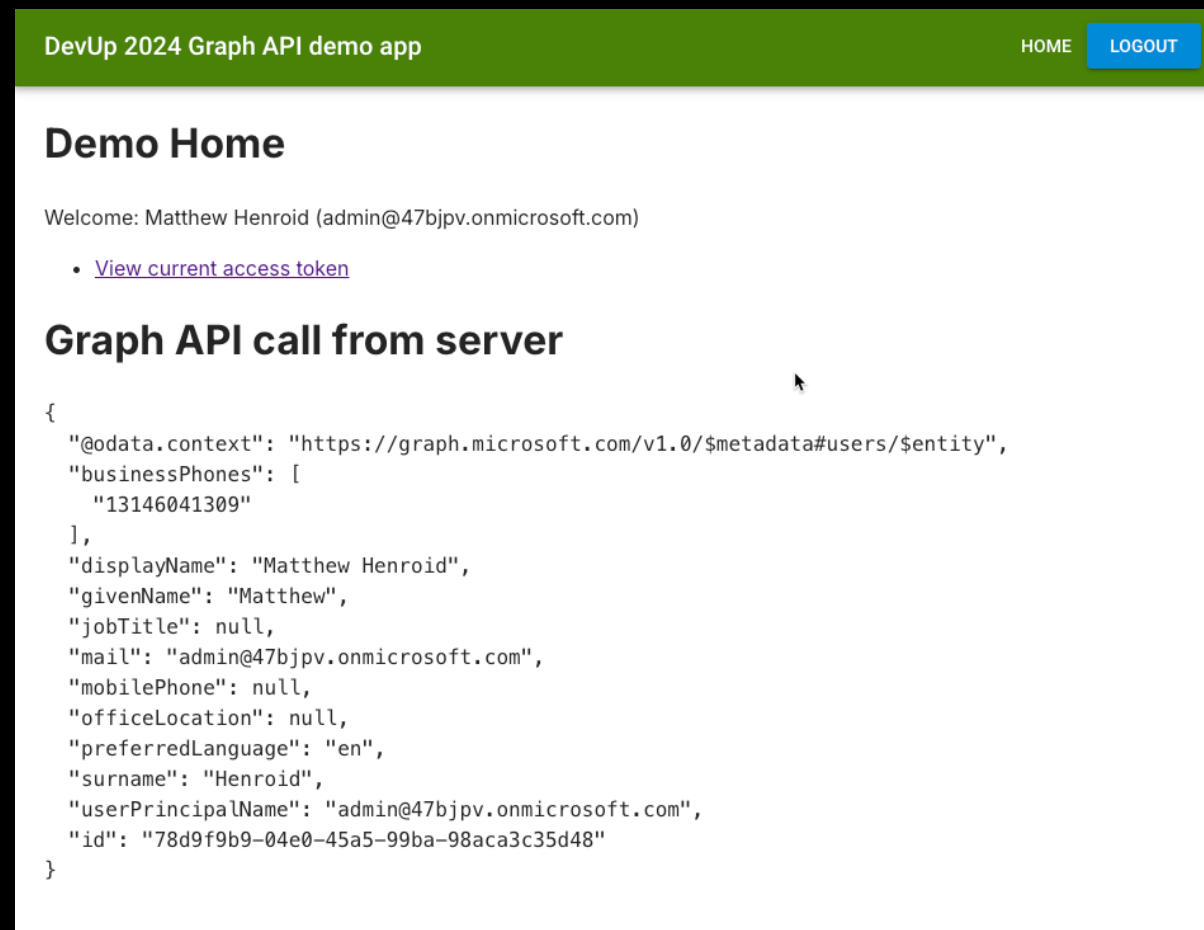
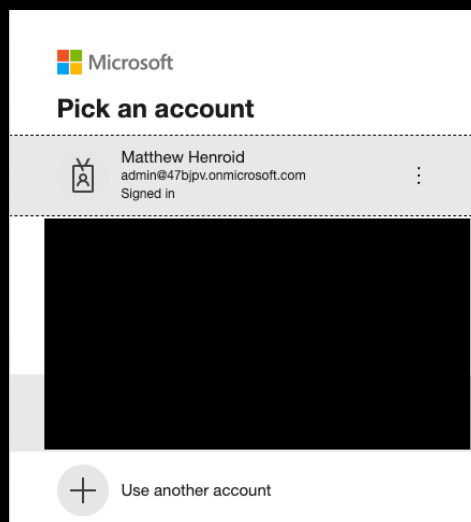
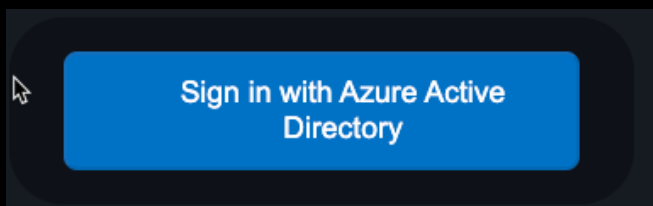
```
1.  
"app_displayname": "Graph Explorer",  
"appid": "de8bc8b5-d9f9-48b1-a8ad-b748da725064",  
"appidacr": "0",  
"family_name": "Henroid",  
"given_name": "Matthew",  
"scp": "openid profile Sites.Read.All User.Read email",
```

Demo App

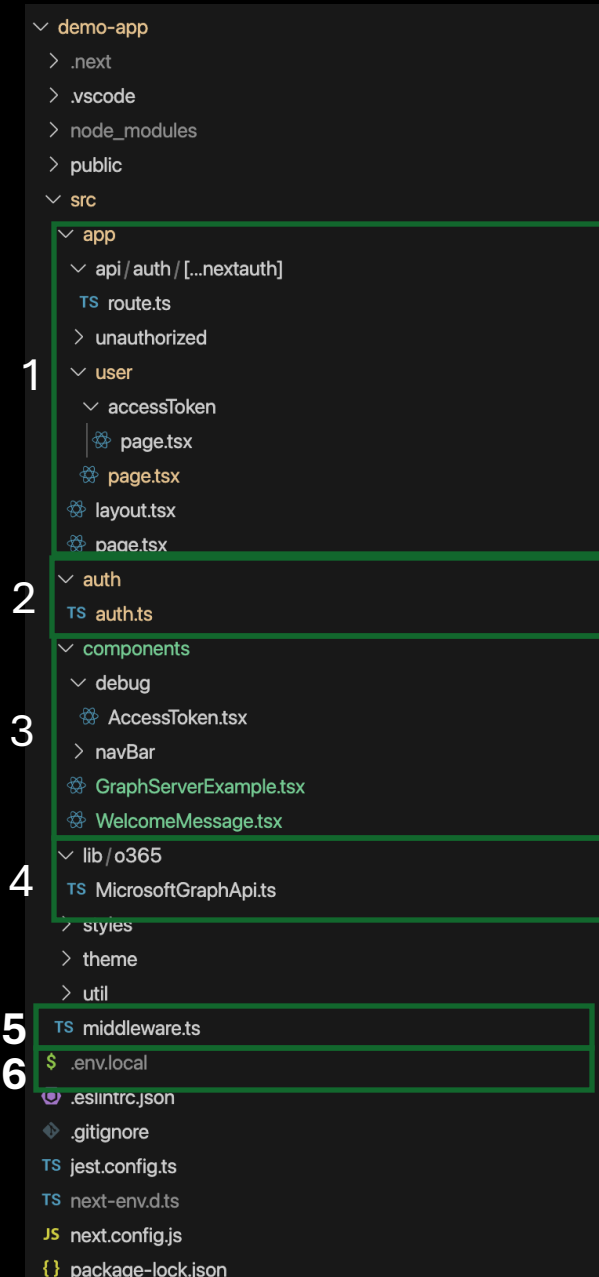
Creating a custom app to access Graph data

Demo App

- Uses Next.js hosted on web server (confidential app)
- Uses NextAuth library to manage authentication



Demo App



1. File based routing, pages, layouts and /api routes (authorization)
2. NextAuth library configurations
3. Various React components used in pages
4. Helper class that handles communication with Microsoft Graph Client via the @microsoft/microsoft-graph-client Node library.
5. Middleware that handles authentication using NextAuth library
6. Env file where we store all our configurations and secrets. Not checked into source control!

```
1 AZURE_AD_CLIENT_ID=  
2 AZURE_AD_CLIENT_SECRET=  
3 AZURE_AD_TENANT_ID=  
4 AZURE_AD_SCOPES=openid profile email offline_access Directory.Read.All Files.Read.All User.Read  
5 NEXTAUTH_SECRET=  
6 NEXTAUTH_URL=http://localhost:3000  
7
```

App Registration

Registering our app with Microsoft

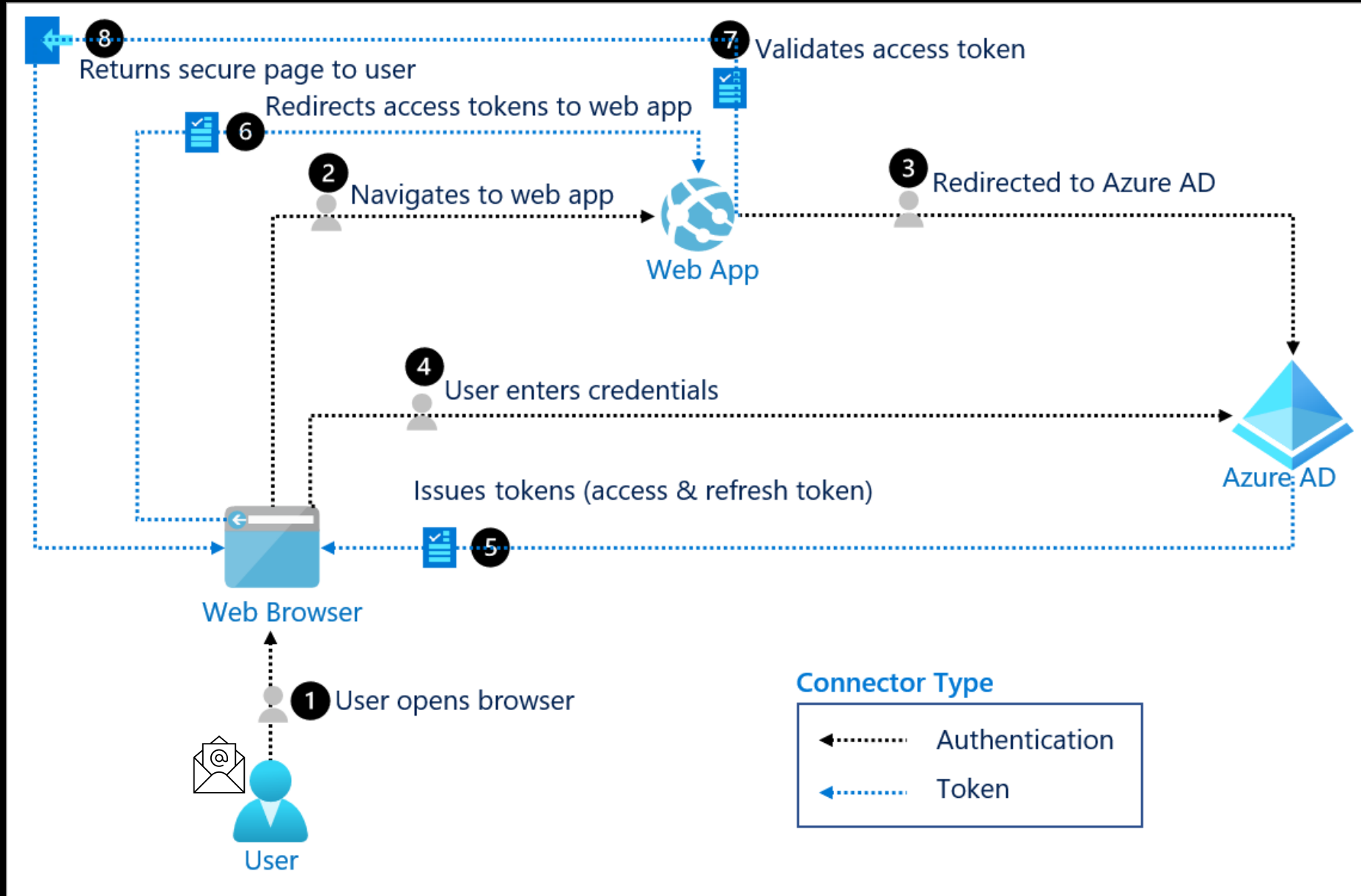
App Registration

The type of authentication flow is dependent on the type of app we're building

App Type	Available Authentication Flows	Notes
Web App on Server	<ul style="list-style-type: none">• OAuth 2.0 authorization code flow	Only for Confidential Applications (OAuth app secret must be stored on server).
Single Page App (SPA)	<ul style="list-style-type: none">• OAuth 2.0 authorization code + Proof Key for Code Exchange (PKCE)• OAuth 2.0 implicit grant flow	Cannot be trusted with app secret
Native / Mobile app	<ul style="list-style-type: none">• OAuth 2.0 authorization code + Proof Key for Code Exchange (PKCE)	Device installed apps similar security to SPA. Also cannot be trusted with an app secret.
Server, daemons and scripts	<ul style="list-style-type: none">• OAuth 2.0 client credentials grant flow	Uses its own credentials instead of impersonating a user

We'll use OAuth 2.0 authorization code flow since our Web App is hosted on a web server and can be trusted with our App Registration secret

OAuth 2.0 authorization code flow

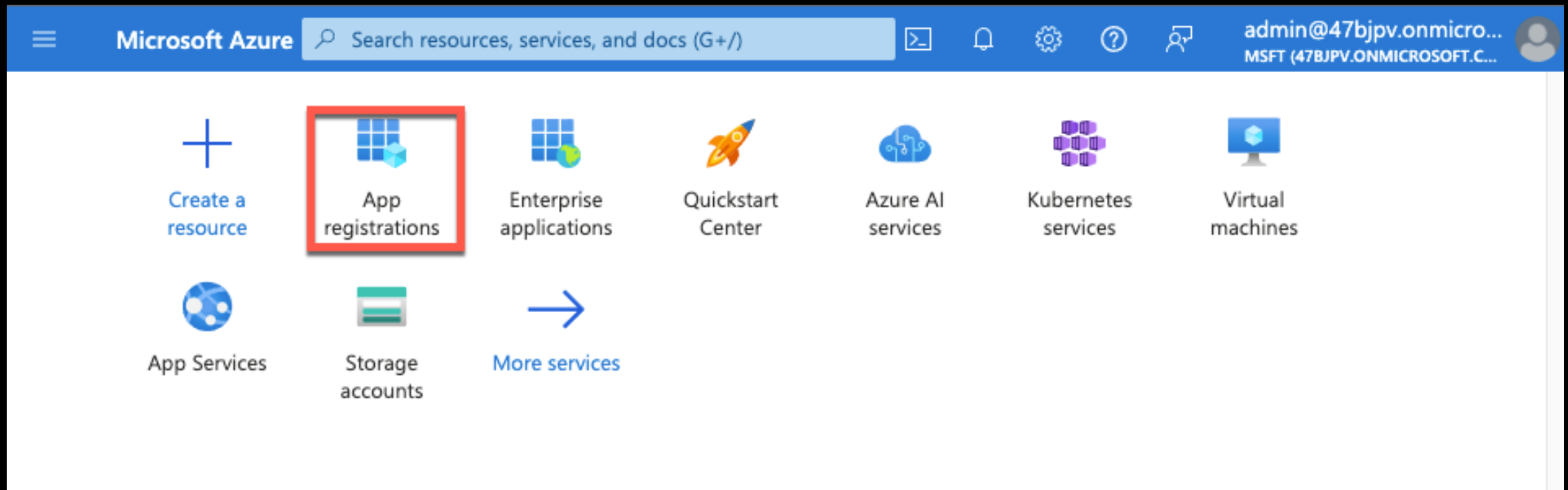


App Registration

<https://portal.azure.com>

Here's an article on how to create a Development O365 Tenant

<https://medium.com/@antoniosql/how-to-get-a-microsoft-365-demo-tenant-8381d712b305>



App Registration

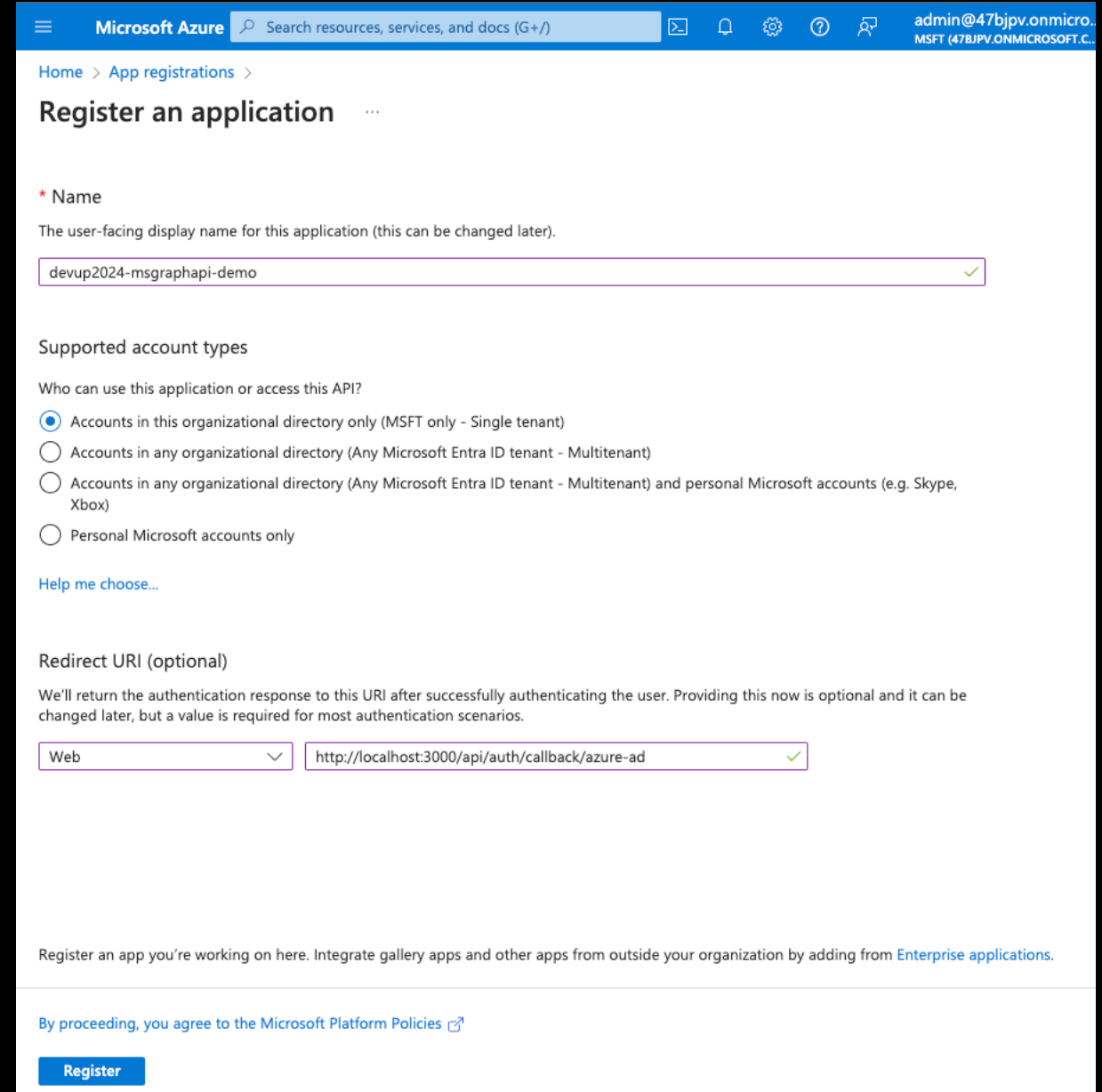
Choose New registration

The screenshot shows the Microsoft Azure portal interface for App Registrations. The top navigation bar includes the Microsoft Azure logo, a search bar, and user information for 'admin@47bjpv.onmicro...'. The main heading is 'App registrations'. Below the heading, there is a row of links: '+ New registration' (highlighted with a red box), 'Endpoints', 'Troubleshoot', 'Refresh', 'Download', 'Preview features', and 'Got feedback?'. A light blue information banner states: 'Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure Active Directory Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. [Learn more](#)'. Below the banner, there are tabs for 'All applications', 'Owned applications' (selected), and 'Deleted applications'. A search bar prompts the user to 'Start typing a display name or application (client) ID to filter these r...'. To the right of the search bar is an 'Add filters' button. At the bottom, a message states: 'This account isn't listed as an owner of any applications in this directory.' Below this message is a blue button labeled 'View all applications in the directory'.

App Registration

- Choose a name for your app
- Choose whether app can be used only on this tenant or multiple
- Choose 'Web' and enter Redirect URI

`http://localhost:3000/api/auth/callback/azure-ad`



The screenshot shows the 'Register an application' page in the Microsoft Azure portal. The page is titled 'Register an application' and is part of the 'App registrations' section. It contains the following fields and options:

- Name:** A text input field with the value 'devup2024-msgraphapi-demo' and a green checkmark icon on the right.
- Supported account types:** A section titled 'Who can use this application or access this API?' with four radio button options:
 - ☒ Accounts in this organizational directory only (MSFT only - Single tenant)
 - ☐ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)
 - ☐ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
 - ☐ Personal Microsoft accounts only
- Help me choose...** A link below the account type options.
- Redirect URI (optional):** A section with a description: 'We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.' It contains two input fields:
 - A dropdown menu with 'Web' selected.
 - A text input field with the value 'http://localhost:3000/api/auth/callback/azure-ad' and a green checkmark icon on the right.
- Footer:** A link 'By proceeding, you agree to the Microsoft Platform Policies' and a blue 'Register' button.


App Registration

- Save the Application ID
- Save the Directory (tenant) ID
- Click *Add a client or secret*

The screenshot displays the Microsoft Azure portal interface for an application registration. The top navigation bar includes the 'Microsoft Azure' logo, a search bar, and user information for 'admin@47bjpv.onmicro...'. The breadcrumb trail shows 'Home > App registrations > devup2024-msgraphapi-demo'. The left sidebar contains navigation links: 'Overview' (selected), 'Quickstart', 'Integration assistant', 'Diagnose and solve problems', 'Manage', and 'Support + Troubleshooting'. The main content area is divided into two columns. The left column, titled 'Essentials', lists key identifiers: 'Display name' (devup2024-msgraphapi-demo), 'Application (client) ID' (redacted), 'Object ID' (d34831ec-d8e0-405e-a962-53cba62066d6), 'Directory (tenant) ID' (redacted), and 'Supported account types' (My organization only). The right column, titled 'Client credentials', contains a red-bordered box around the 'Add a certificate or secret' link, along with 'Redirect URIs' (1 web, 0 spa, 0 public client), 'Application ID URI' (Add an Application ID URI), and 'Managed application in local directory' (devup2024-msgraphapi-demo).


App Registration


- Click *New client secret*

 Application registration certificates, secrets and federated credentials can be found in the tabs below.

Certificates (0) Client secrets (0) Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

 New client secret

Description	Expires	Value 	Secret ID
No client secrets have been created for this application.			

App Registration


- Enter a description and expiration date
- Save


Add a client secret ✕

Description	<input type="text" value="main"/>
Expires	<input type="text" value="730 days (24 months)"/> ✓


App Registration

- Copy the generated secret value (not Secret ID)
- This is the last time you'll be able to access it!

 Got feedback?

 Got a second to give us some feedback? →

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.


 Application registration certificates, secrets and federated credentials can be found in the tabs below.



Certificates (0)

Client secrets (1)

Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

 New client secret

Description	Expires	Value ⓘ	Secret ID
main	8/11/2026	AeT8Q~IP9h7hUcYkd3tXaehoL5...	c09c92cb-d31e-4268-bf71-56f88...  

App Registration

- Navigate to the API permissions tab
- User.Read is available by default
- We also want Files.Read.All and Directory.Read.All
- Click *Add a permission*

The screenshot shows the 'API permissions' page in the Azure AD portal for the application 'devup2024-msgraphapi-demo'. The left sidebar contains navigation links: Overview, Quickstart, Integration assistant, Diagnose and solve problems, Manage (expanded), Branding & properties, Authentication, Certificates & secrets, Token configuration, API permissions (selected), Expose an API, App roles, Owners, Roles and administrators, Manifest, and Support + Troubleshooting. The main content area has a search bar, 'Refresh' button, and 'Got feedback?' link. It displays two informational banners: a warning about tenant-wide consent and an info note about the 'Admin consent required' column. Below these is the 'Configured permissions' section, which includes a link to 'Add a permission' and a checkmark for 'Grant admin consent for MSFT'. A table lists the configured permissions for 'Microsoft Graph (1)'. The table has columns for 'API / Permissions name', 'Type', 'Description', 'Admin consent requ...', and 'Status'. One permission is listed: 'User.Read' with a 'Delegated' type and description 'Sign in and read user profile'. The 'Admin consent required' is 'No'. At the bottom, a note states: 'To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try [Enterprise applications](#).'

API / Permissions name	Type	Description	Admin consent requ...	Status
▼ Microsoft Graph (1)				
User.Read	Delegated	Sign in and read user profile	No	...

App Registration


- Choose Microsoft Graph

Request API permissions

Select an API


Microsoft APIs APIs my organization uses My APIs

Commonly used Microsoft APIs




Microsoft Graph

Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Microsoft Entra ID, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.




Azure Rights Management Services

Allow validated users to read and write protected content



Azure Service Management

Programmatic access to much of the functionality available through the Azure portal



Dynamics CRM


Access the capabilities of CRM business software and ERP systems

App Registration

- Choose *Delegated permissions*
- Application permissions are only for background services or daemons where user will not login.
- Search for and select Files.Read.All and Directory.Read.All
- Click Add permissions

Request API permissions

[← All APIs](#)

 Microsoft Graph
<https://graph.microsoft.com/> [Docs](#) [↗](#)

What type of permissions does your application require?


Delegated permissions


Your application needs to access the API as the signed-in user.

Application permissions

Your application runs as a background service or daemon without a signed-in user.

Select permissions [expand all](#)

 Start typing a permission to filter these results

 The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in your organization, or in organizations where this app will be used. [Learn more](#)

Permission	Admin consent required
▼ OpenId permissions	
<input type="checkbox"/> email ⓘ View users' email address	No
<input type="checkbox"/> offline_access ⓘ Maintain access to data you have given it access to	No
<input type="checkbox"/> openid ⓘ Sign users in	No
<input type="checkbox"/> profile ⓘ View users' basic profile	No
> AccessReview	

Add permissionsDiscard

App Registration

- Some permissions require Admin consent to enable
- If you are an Admin for your tenant you can do this yourself
- Click Grant admin consent for <TENANT>
- Grant consent

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission

☒ Grant admin consent for MSFT

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (3)				
Directory.Read.All	Delegated	Read directory data	Yes	⚠ Not granted for MSFT
Files.Read.All	Delegated	Read all files that user can access	No	
User.Read	Delegated	Sign in and read user profile	No	

Grant admin consent confirmation.

Do you want to grant consent for the requested permissions for all accounts in MSFT? This will update any existing admin consent records this application already has to match what is listed below.

Yes

No

After consent

he consent process. The list of configured permissions should include

Admin consent requ...	Status
Yes	✔ Granted for MSFT
No	✔ Granted for MSFT
No	✔ Granted for MSFT

Run the App

Using our web server to access Microsoft Graph data

Configure App

- Copy / Rename .env.sample to .env.local
- Enter the Azure client id, client secret and tenant id
- Use openssl to generate a secret for NEXTAUTH_SECRET
- Run the app using 'npm run dev'

```
1  # Copy this file and rename .env.local or .env.development
2  # Do not check these files into source control!
3
4  # The App ID presented immediately after registering your App
5  AZURE_AD_CLIENT_ID=
6
7  # A secret that you must generate when registering your App.
8  AZURE_AD_CLIENT_SECRET=
9
10 # Your Tenant ID. Visible after you create a new App Registration
11 AZURE_AD_TENANT_ID=
12
13 # The scopes listed after offline_access should match exactly with what was registered in
14 # Make sure you keep openid profile email and offline_access
15 AZURE_AD_SCOPES=openid profile email offline_access Directory.Read.All Files.Read.All User.Read
16
17 # Generate using 'openssl rand -base64 32'
18 NEXTAUTH_SECRET=
19
20 # The Base URL for the web application
21 NEXTAUTH_URL=http://localhost:3000
22
23
```

Calling the Graph API

/src/components/GraphServerExample.tsx

```
1 import { useSession } from "next-auth/react";
2 import {
3   AccessTokenAuthProvider,
4   MicrosoftGraphApi,
5 } from "@/lib/o365/MicrosoftGraphApi";
6 import { getAuthSession } from "@/auth/auth";
7
8 export default async function GraphServerExample() {
9   // Get the access token from session state
10  let session = await getAuthSession();
11  let accessToken = session.access_token;
12
13  // Initialize our wrapper class
14  let graphApi = new MicrosoftGraphApi(
15    new AccessTokenAuthProvider(accessToken)
16  );
17
18  // Simple example
19  let result = await graphApi.getJson("https://graph.microsoft.com/v1.0/me");
20
21  // Demonstrate paged results--
22
23  return (
24    <>
25      <h1>Graph API call from server</h1>
26      <pre>{JSON.stringify(result, undefined, 2)}</pre>
27    </>
28  );
29}
```

/src/lib/o365/MicrosoftGraphApi.ts

```
export class MicrosoftGraphApi {
  private authProvider: AuthenticationProvider;

  constructor(authProvider: AuthenticationProvider) {
    if (!authProvider) {
      throw new Error("Missing authProvider parameter");
    }
    this.authProvider = authProvider;
  }

  private getClient(): Client {
    let clientOptions: ClientOptions = {
      authProvider: this.authProvider,
    };
    const client = Client.initWithMiddleware(clientOptions);
    return client;
  }

  public async getJson(url: string): Promise<any> {
    let client = this.getClient();
    let response = await client.api(url).responseType(ResponseType.RAW).get();
    if (response.status === 401) {
      let result = await response.json();
      throw new Error("Unauthorized", { cause: result });
    }
    if (response.ok) {
      return await response.json();
    }
    return null;
  }

  public async get(url: string): Promise<Response> { ... }
  public async post(url: string, content: any): Promise<Response> { ... }
  public async delete(url: string): Promise<Response> { ... }
  public async patch(url: string, content: any): Promise<Response> { ... }
}
```

Q&A