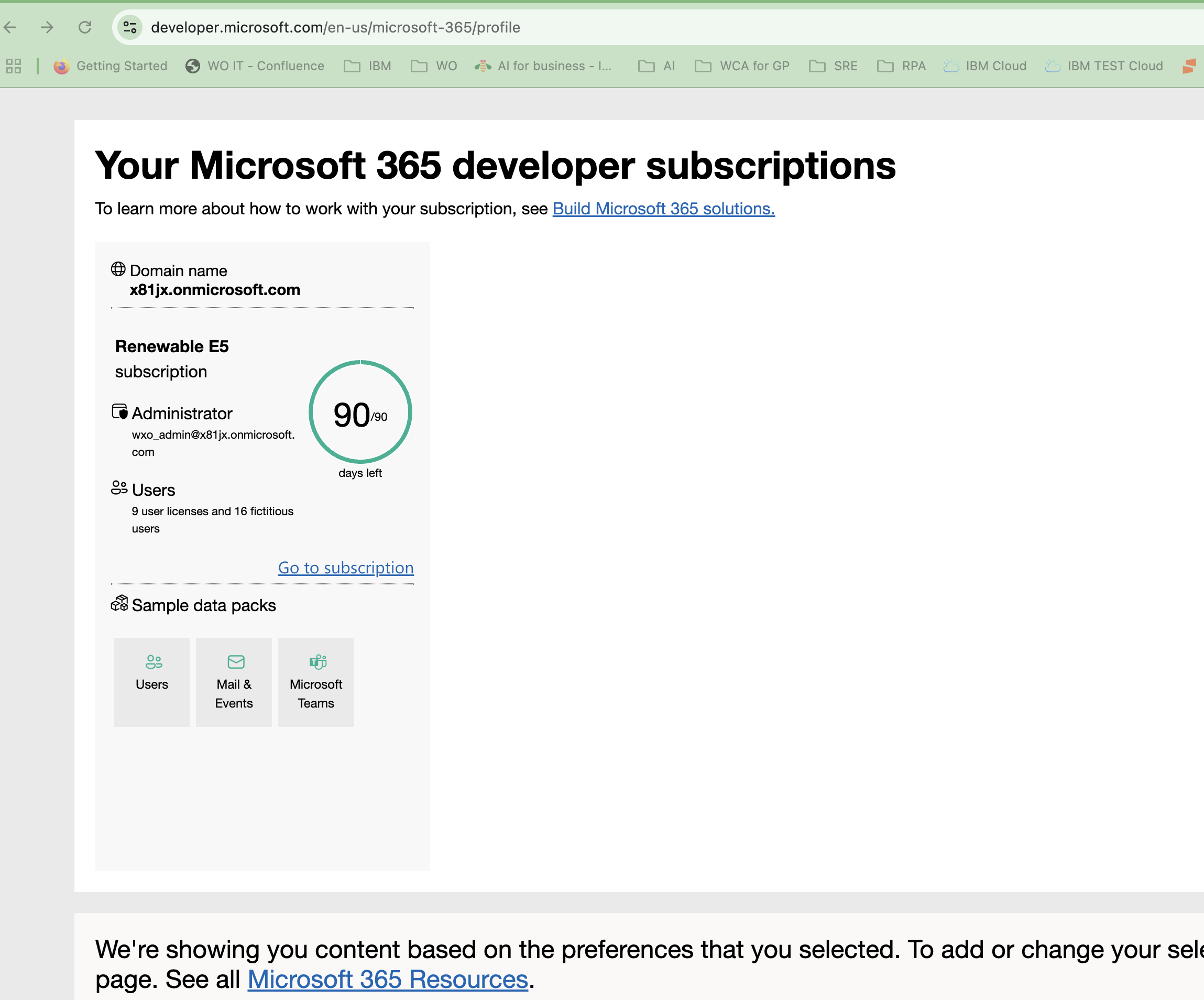
To connect with a **Microsoft 365 (Entra ID / Azure AD)** user management system (like what you access through [admin.microsoft.com](https://admin.microsoft.com/)), you typically use the **Microsoft Graph API**.

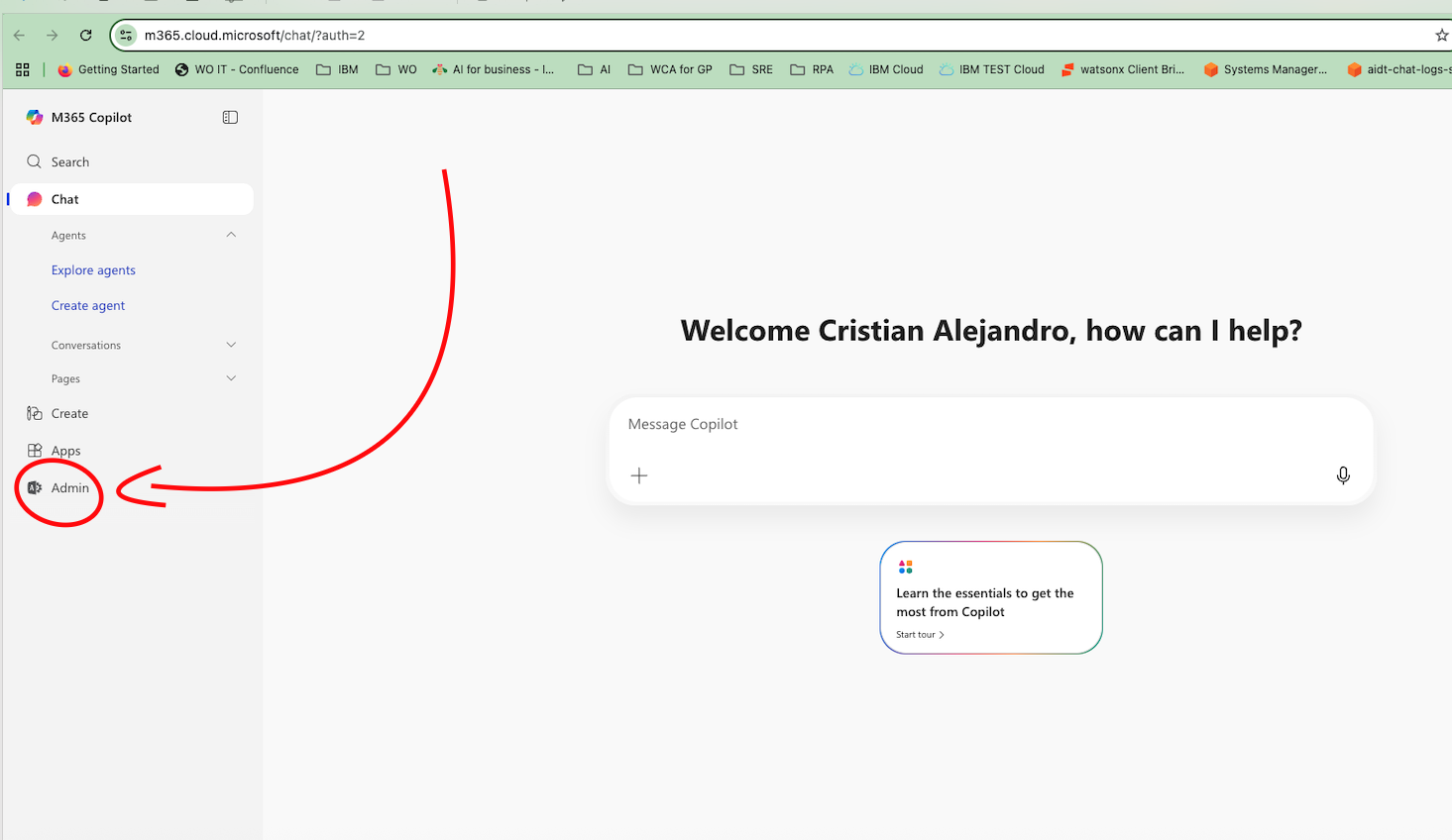
Here’s a step-by-step guide to connect and manage users via REST API using **Microsoft Graph**:

### **Step 1: Join Developer program**

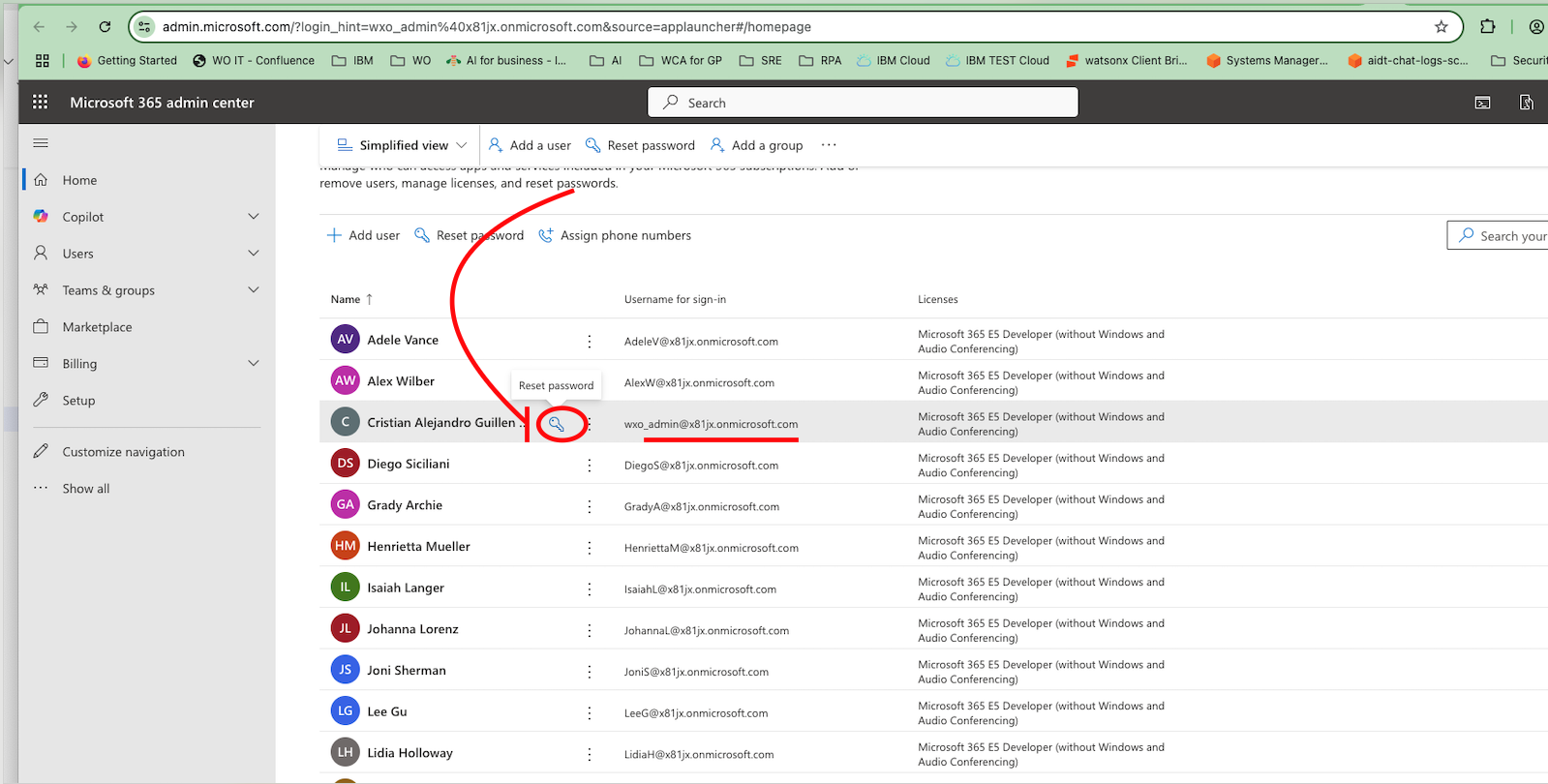
<https://developer.microsoft.com/en-us/microsoft-365/profile>



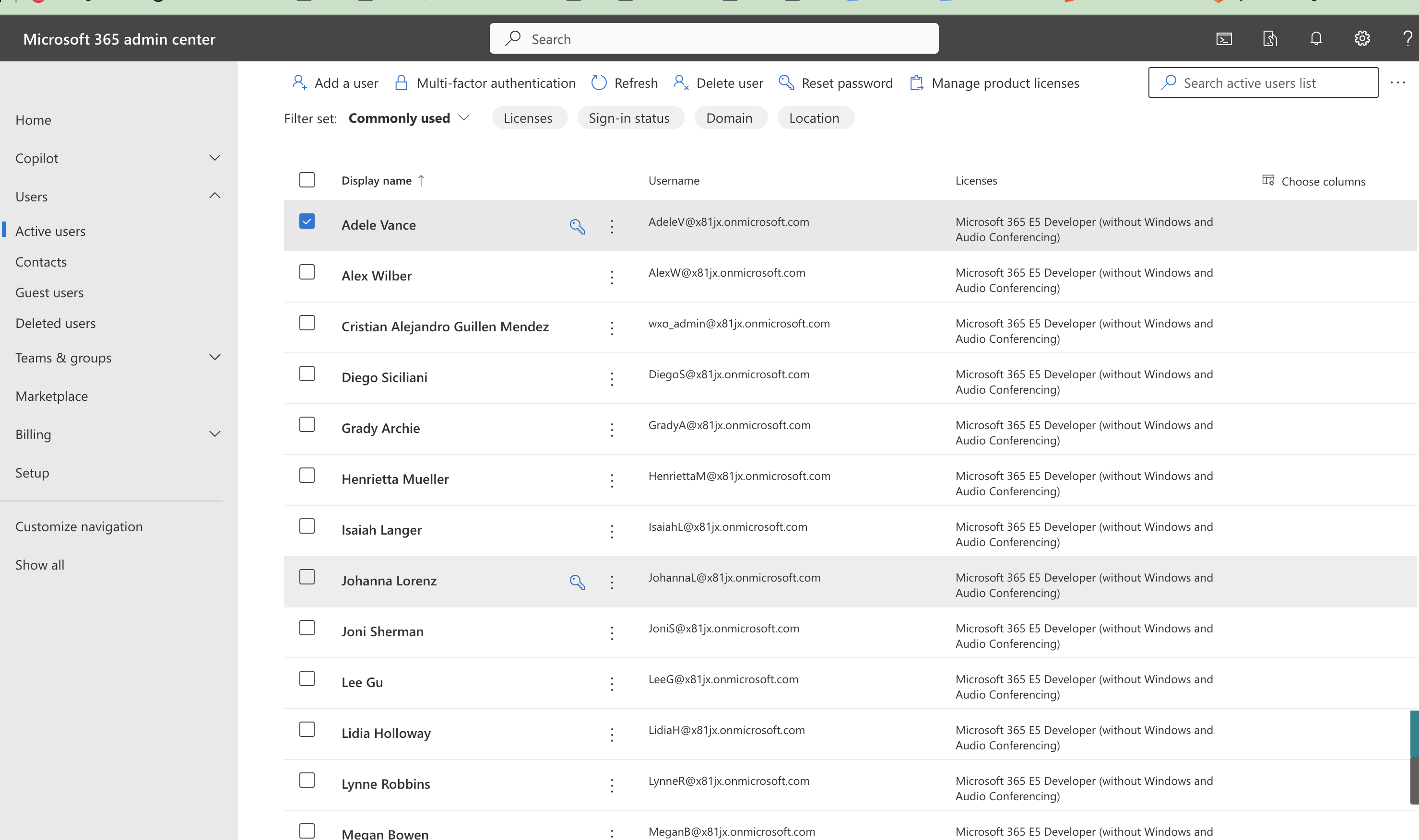


Click “Go to subscription” and then “Admin”

### **Step 1.1: Reset the password for your admin user**

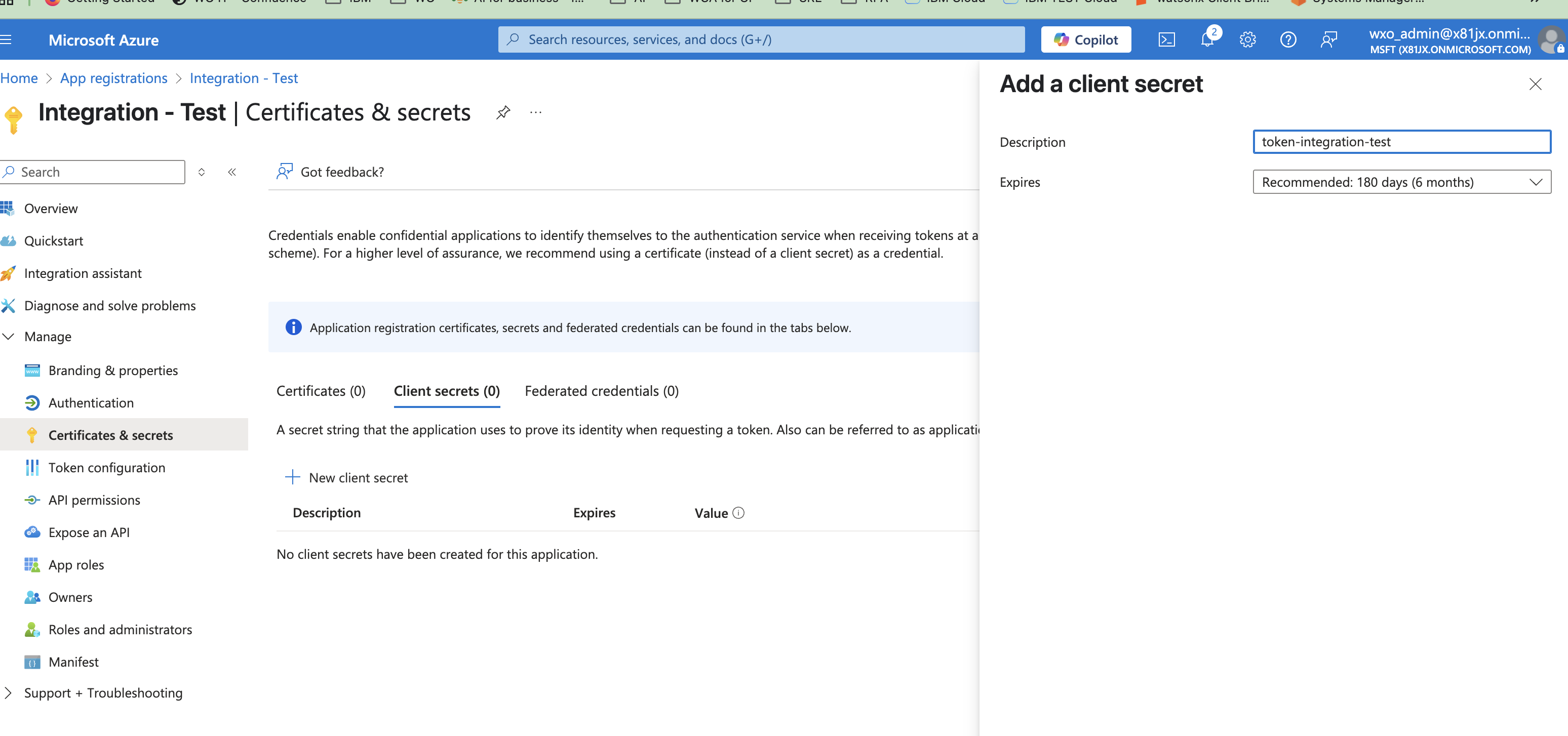
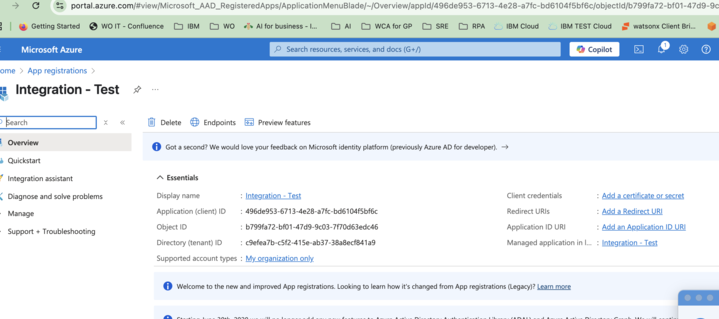
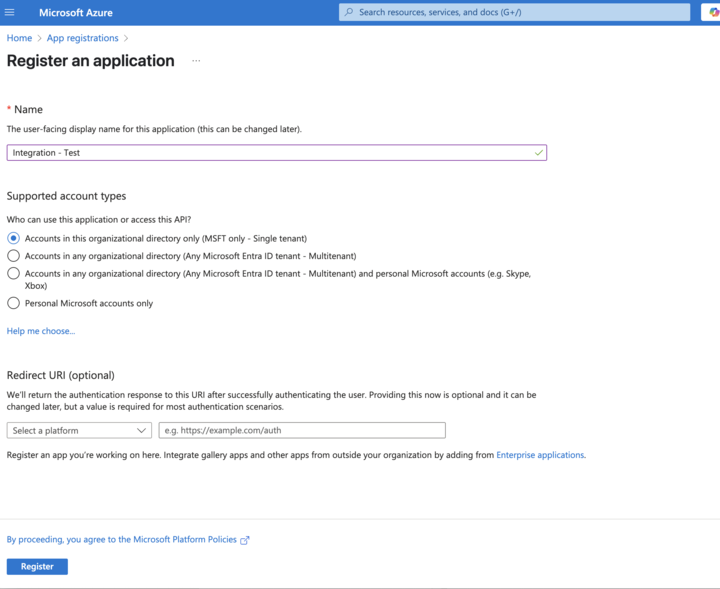
Look for the admin user and reset the password ( we will need it later to login in the app portal)

### **Step 1.2: Enable Active Users**



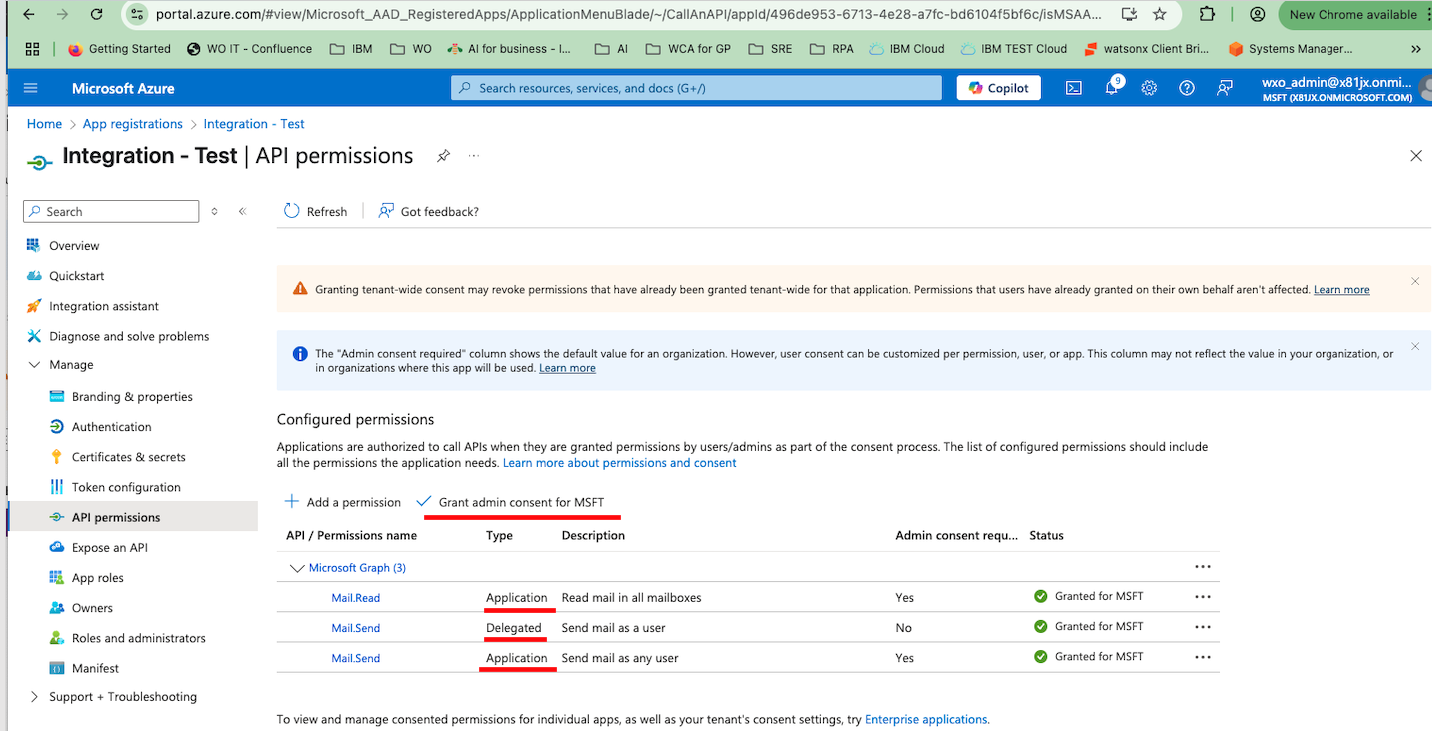
### **Step 2: Register an Application in Azure**

1. Go to [Azure Portal – App Registrations.](https://portal.azure.com/#blade/Microsoft_AAD_RegisteredApps/ApplicationsListBlade) (**use the admin user for the subscription, no your IBM account**)
2. Click **New registration**.
3. Set a name, choose supported account types (usually "Accounts in this organizational directory only").
4. Click **Register**.
5. Note the **Application (client) ID** and **Directory (tenant) ID**.



### **Step 3: Configure API Permissions**

1. Go to your app registration.
2. Navigate to **API permissions** → **Add a permission** → **Microsoft Graph**.
3. Choose:
   1. **Delegated permissions** (if a signed-in user will use the API), or
   2. **Application permissions** (for background/server scripts).
4. For user management, add:
   1. Email.Read
   2. Email.Read
5. Note: Add all permissions based on your use case!!!!!
6. Click **Grant admin consent** for the tenant.
7. The error **"Not granted for MSFT"** appears when your application has requested API permissions, but **admin consent was not granted**, **especially in Microsoft tenants where elevated permissions are tightly controlled (e.g., MSFT-internal tenants or developer tenants).**

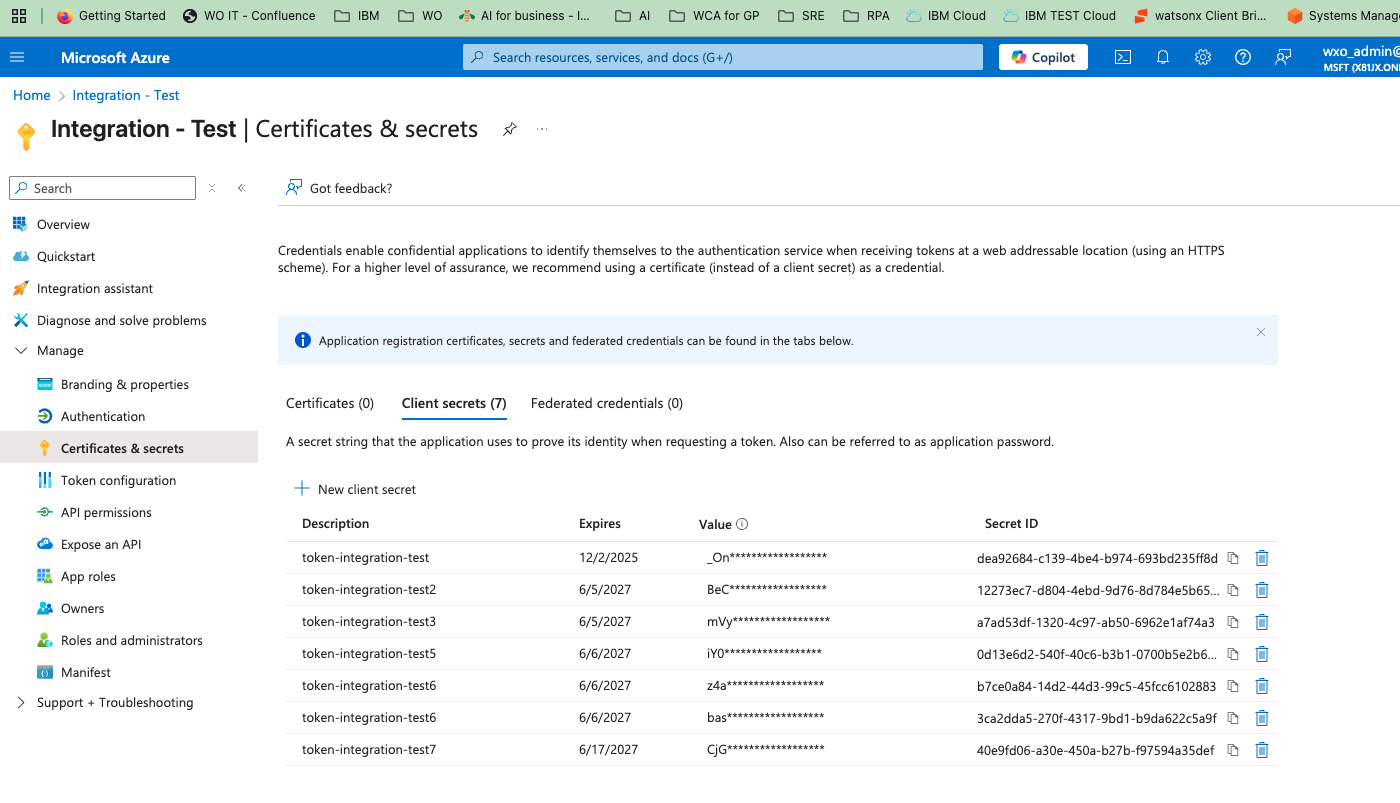


### **Step 4: Create a Client Secret**

1. Go to **Certificates & secrets** → **New client secret**.
2. Copy and save the secret value (you will use this in the token request).

To connect with a **Microsoft 365 (Entra ID / Azure AD)** user management system (like what you access through [admin.microsoft.com](https://admin.microsoft.com/)), you typically use the **Microsoft Graph API**.

Here’s a step-by-step guide to connect and manage users via REST API using **Microsoft Graph**:



### **Step 5: Register an Application in Azure**

1. Go to Azure Portal – App Registrations.
2. Click **New registration**.
3. Set a name, choose supported account types (usually "Accounts in this organizational directory only").
4. Click **Register**.
5. Note the **Application (client) ID** and **Directory (tenant) ID**.

### **Step 8: Get an Access Token (Optional, just to test)**

Use the **OAuth 2.0 client credentials flow** (if using application permissions):

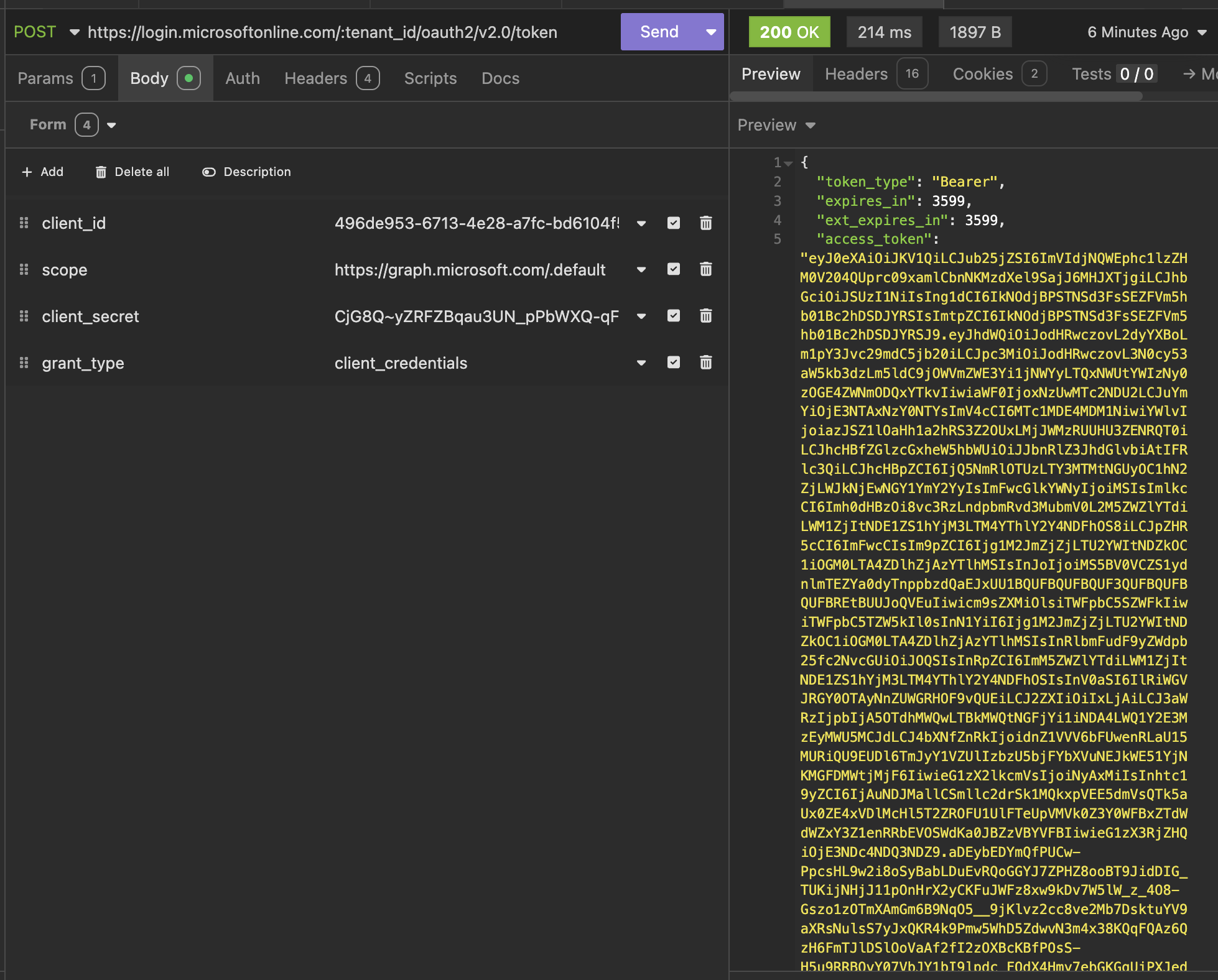
**POST** <https://login.microsoftonline.com/{tenant_id}/oauth2/v2.0/token>

#### **Headers:**

Content-Type: application/x-www-form-urlencoded

#### **Body (x-www-form-urlencoded):**

client\_id=YOUR\_CLIENT\_ID  
&scope=https://graph.microsoft.com/.default  
&client\_secret=YOUR\_CLIENT\_SECRET  
&grant\_type=client\_credentials



### **Step 5: Send email (Optional, just to test)**

Use the access token to call Microsoft Graph API.

#### **Example: List Users**

**GET** <https://graph.microsoft.com/v1.0/users>

#### **Headers:**

Authorization: Bearer YOUR\_ACCESS\_TOKEN

#### **Example: Send email**

**POST** https://graph.microsoft.com/v1.0/users/:sender-user-id-or-upn/sendMail

{

"message": {

"subject": "Hello from Microsoft Graph",

"body": {

"contentType": "Text",

"content": "This is the email body sent from Microsoft Graph API."

},

"toRecipients": [

{

"emailAddress": {

"address": "cguillen@ibm.com"

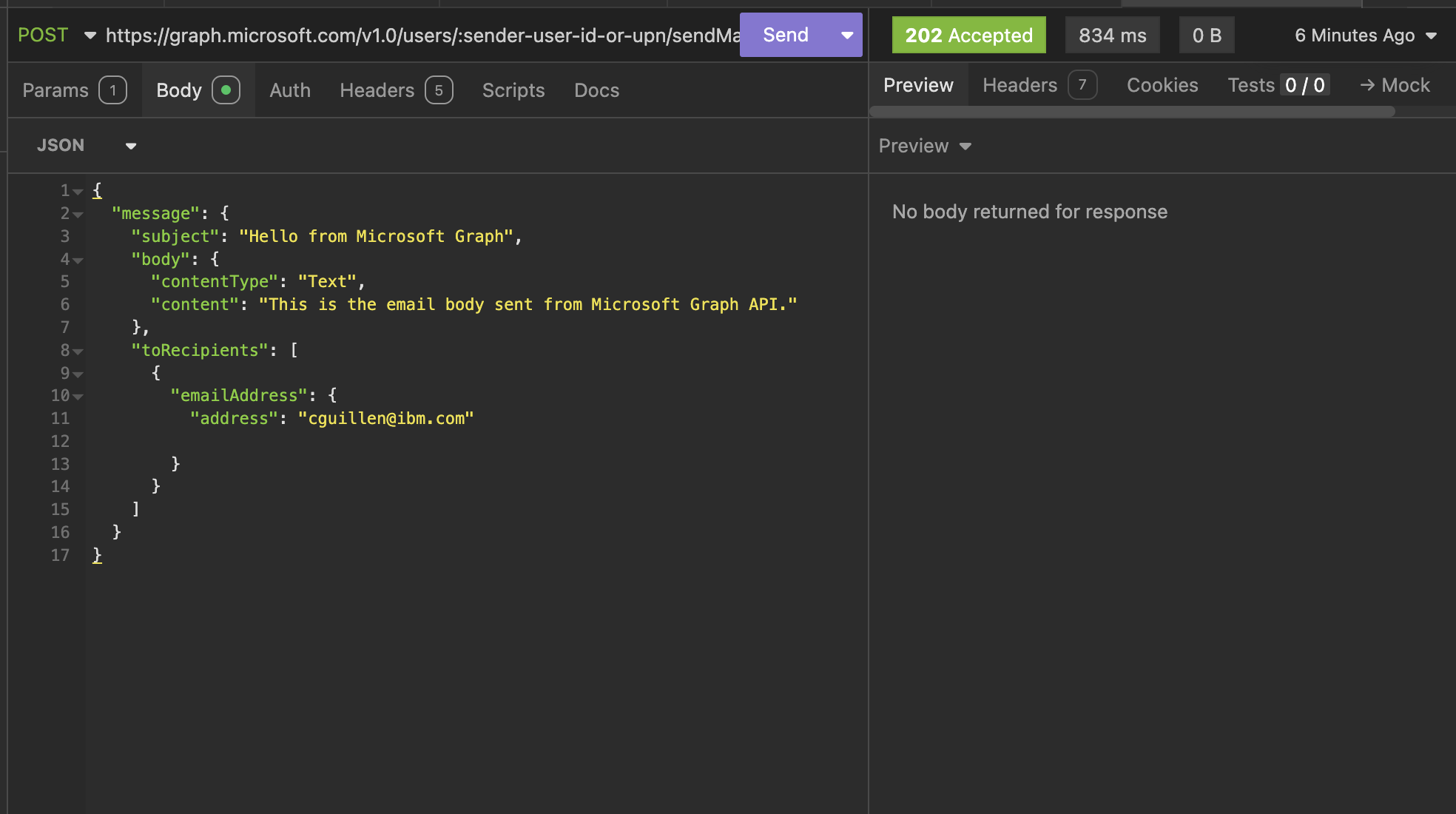
}

}

]

}

}

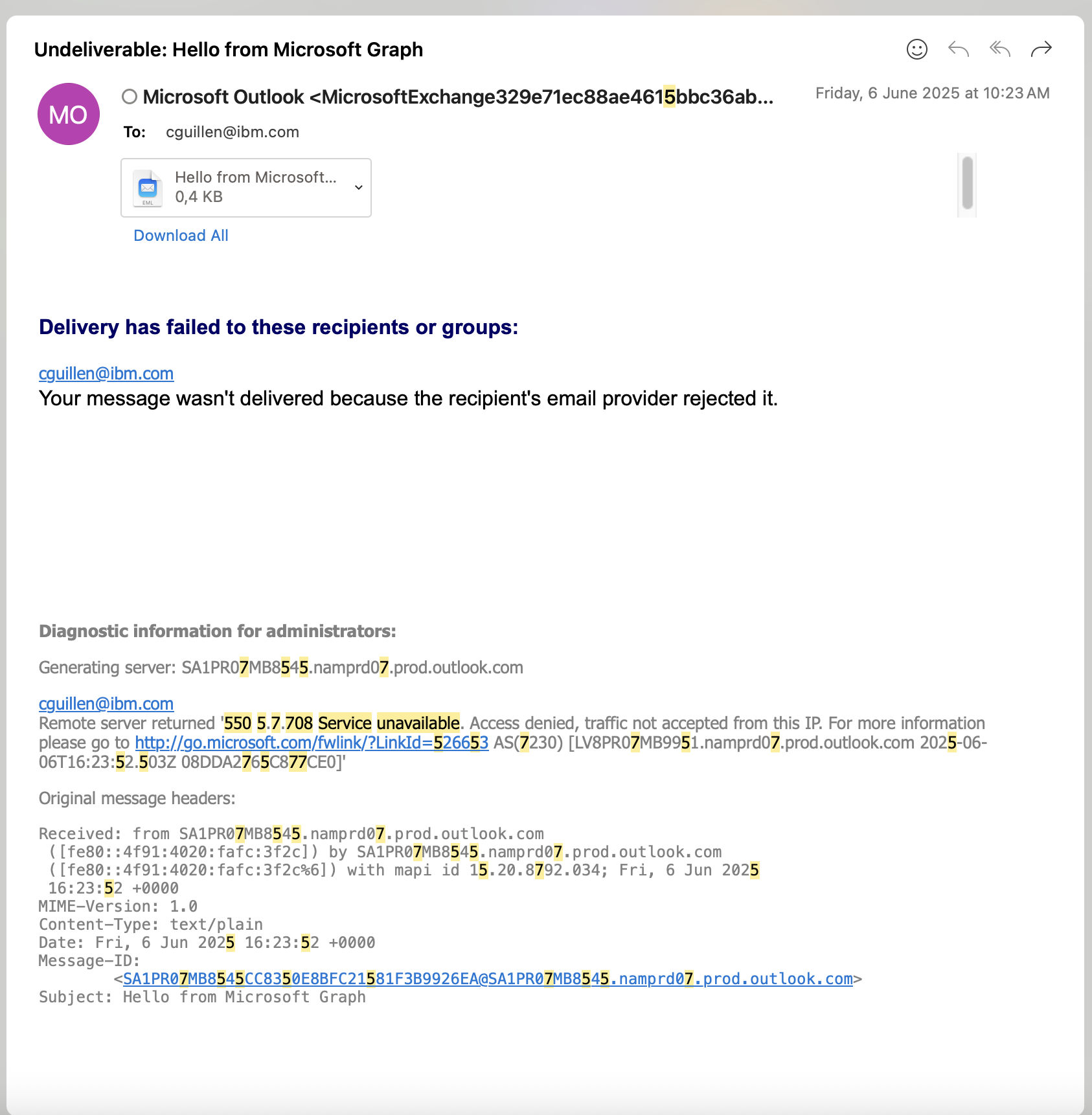


### **❌❌❌❌❌❌❌ Your email was rejected due to anti-spam restrictions on Microsoft 365 tenants.**

Specifically, this part of the error is key:

550 5.7.708 Service unavailable. Access denied, traffic not accepted from this IP.  
For more information please go to <http://go.microsoft.com/fwlink/?LinkId=526653>

That [link](http://go.microsoft.com/fwlink/?LinkId=526653) takes you to the Microsoft Docs page about **restricted outbound mail for newly created tenants**.



## **💡 Why it happens**

Microsoft **restricts outbound email from new tenants** (especially with application-permission-based sendMail) to prevent spam and abuse.

You **can send emails via Outlook**, because that's considered *user-initiated* and follows different anti-abuse policies.

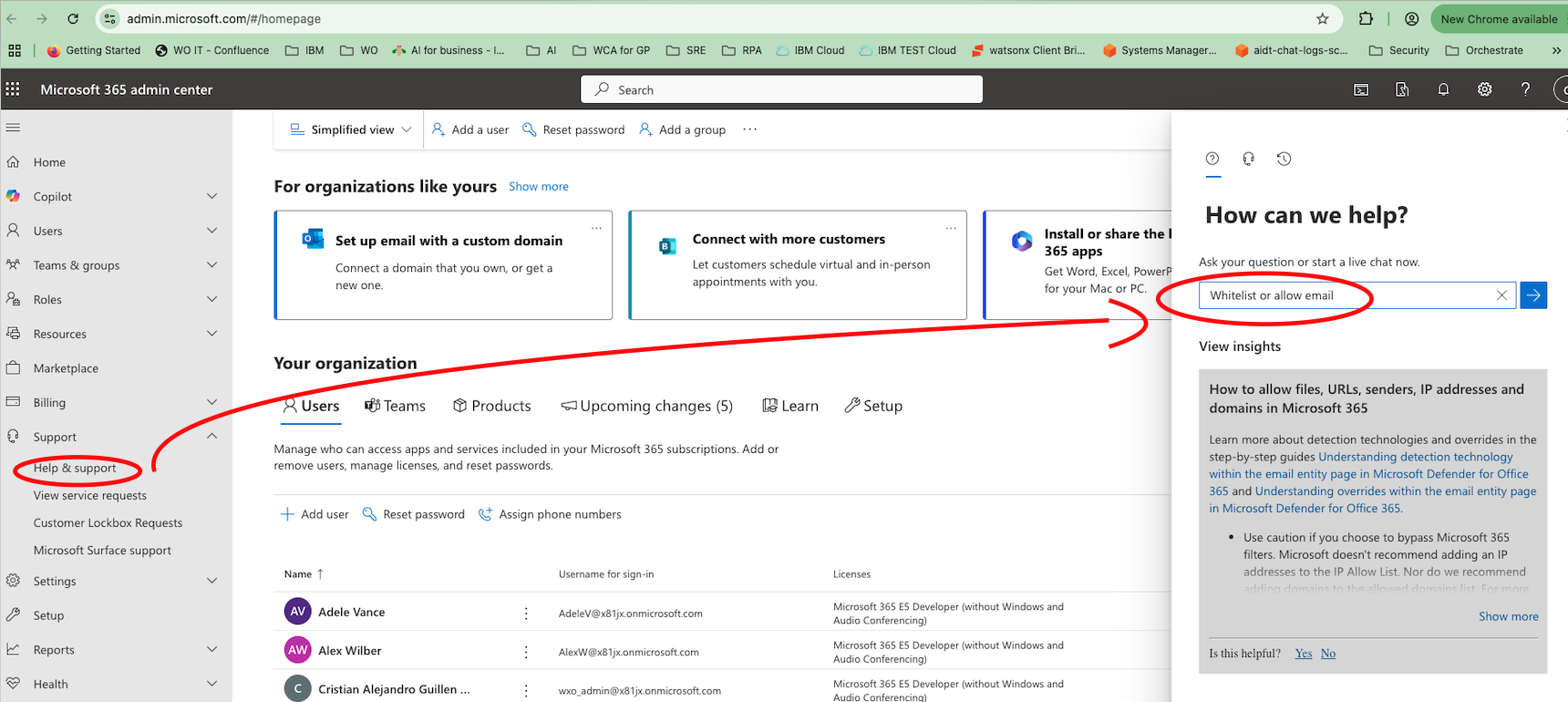
But **emails sent via Microsoft Graph REST API using application permissions** are restricted until Microsoft verifies your tenant and allows outbound traffic.

## **How to fix it**

You must **submit a request to Microsoft support to lift the outbound mail restriction**. Here's how:

### **Step-by-step:**

1. Go to the [**Microsoft 365 Admin Center**](https://admin.microsoft.com/)
2. Click **Support > New service request**



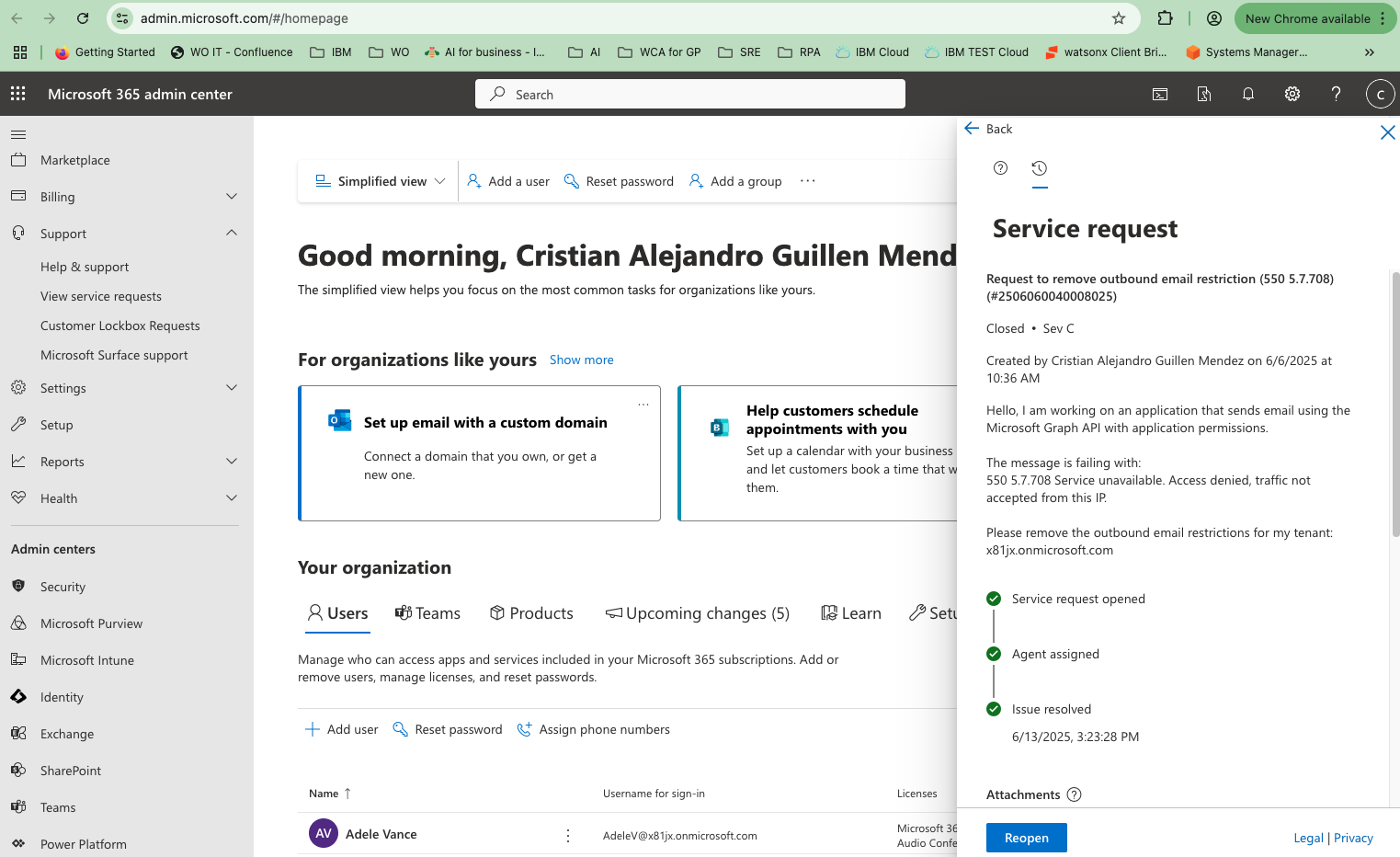
1. Use a subject like:  
    Request to remove outbound email restriction (550 5.7.708)
2. Describe the problem using this template:

Hello, I am working on an application that sends email using the Microsoft Graph API with application permissions.

The message is failing with:  
 550 5.7.708 Service unavailable. Access denied, traffic not accepted from this IP.

Please remove the outbound email restrictions for my tenant: **x81jx.onmicrosoft.com**

1. Submit the ticket and wait for Microsoft to respond — this usually takes **24–48 hours**.



## Tools to Help

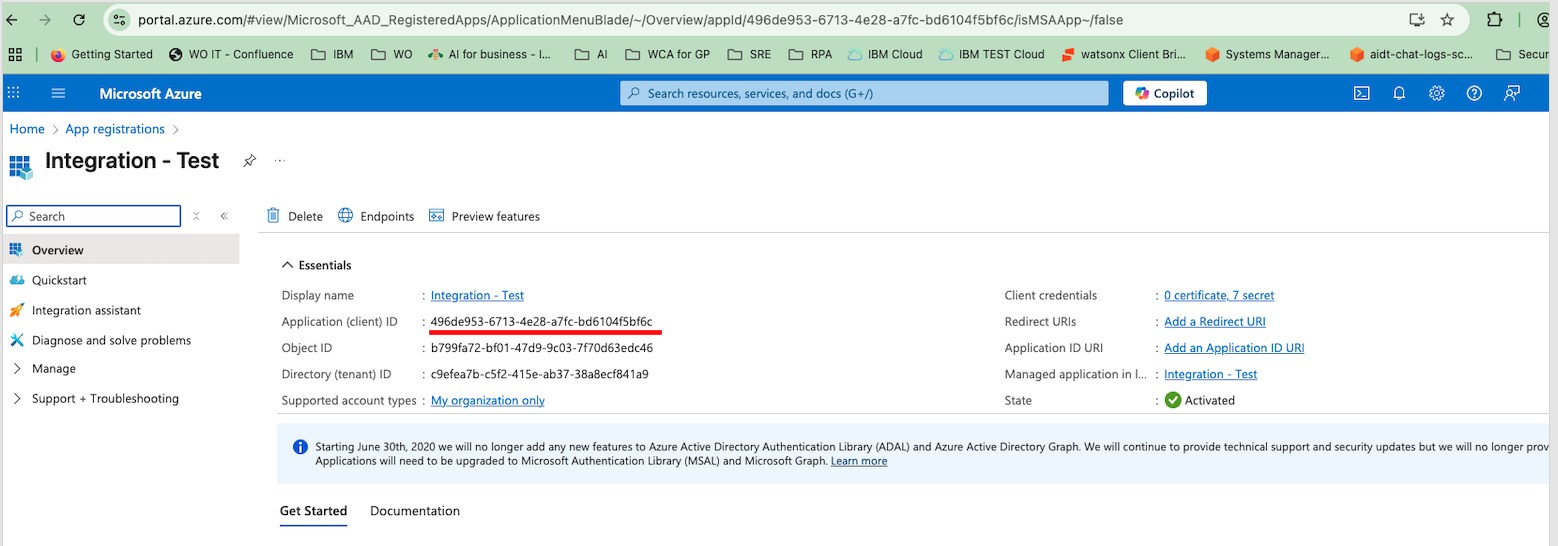
You can test all this easily with:

* [Graph Explorer](https://developer.microsoft.com/en-us/graph/graph-explorer)

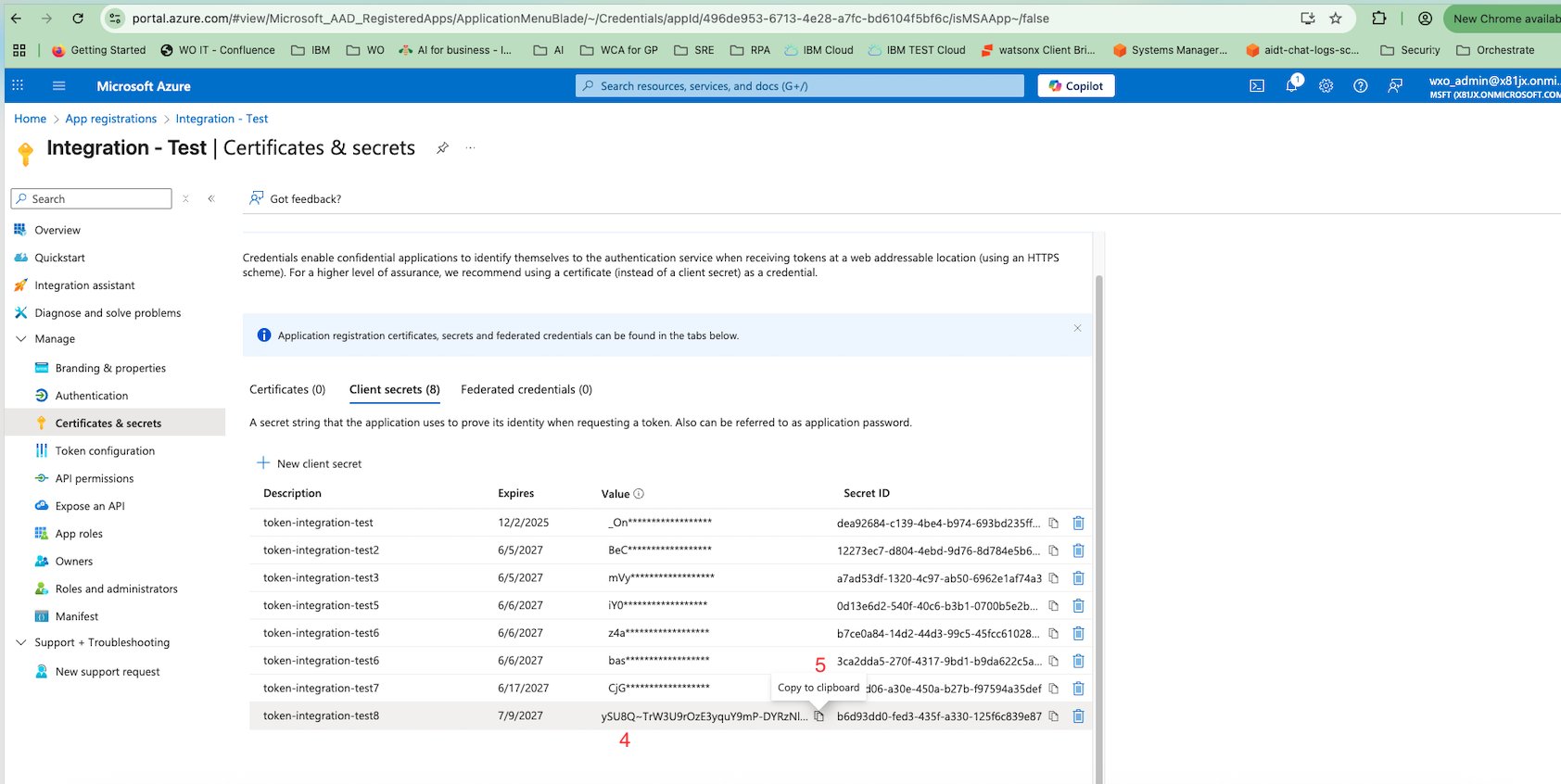
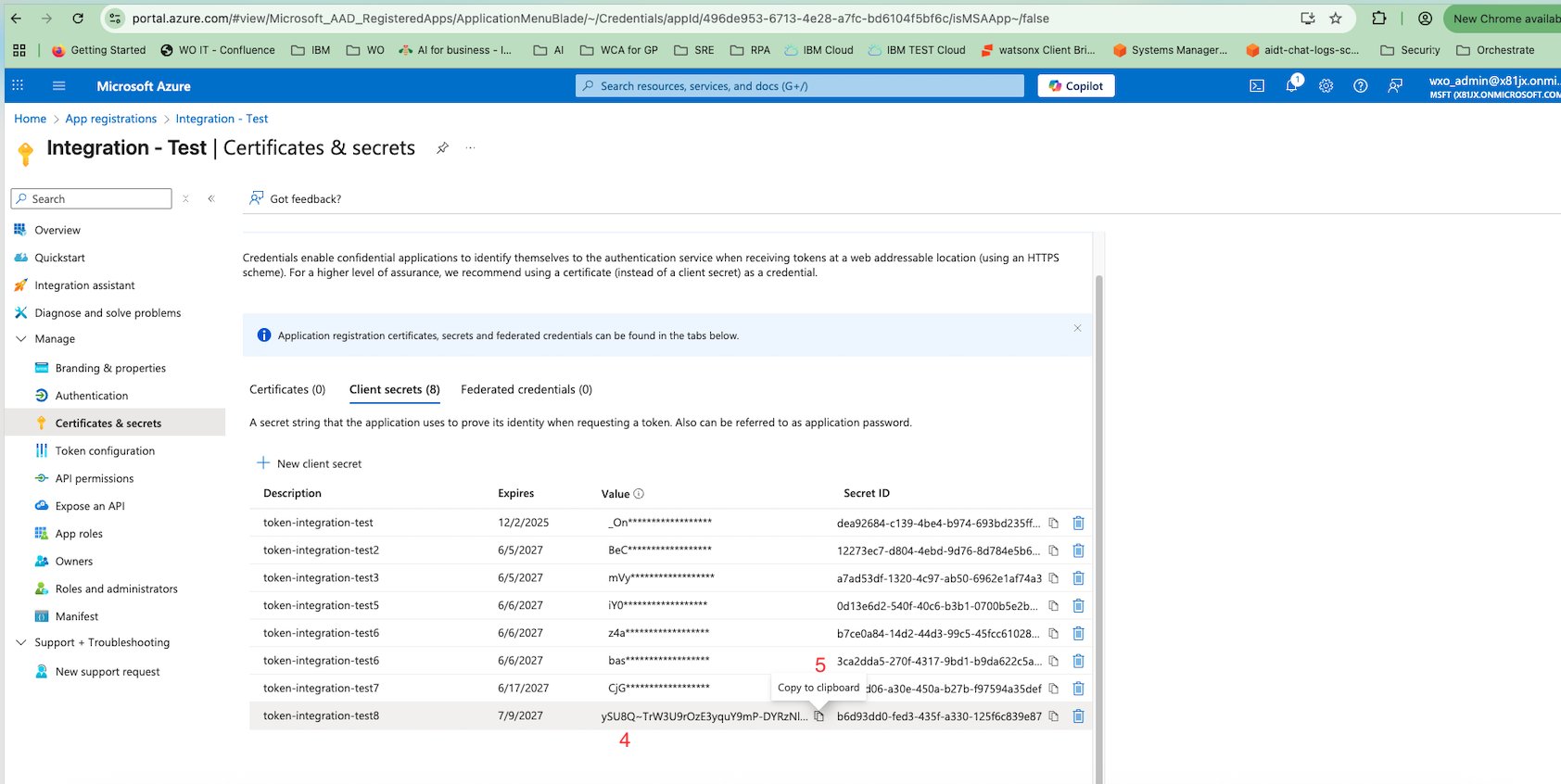
## Orchestrate configuration

You need to create key-value pair in the connection settings:

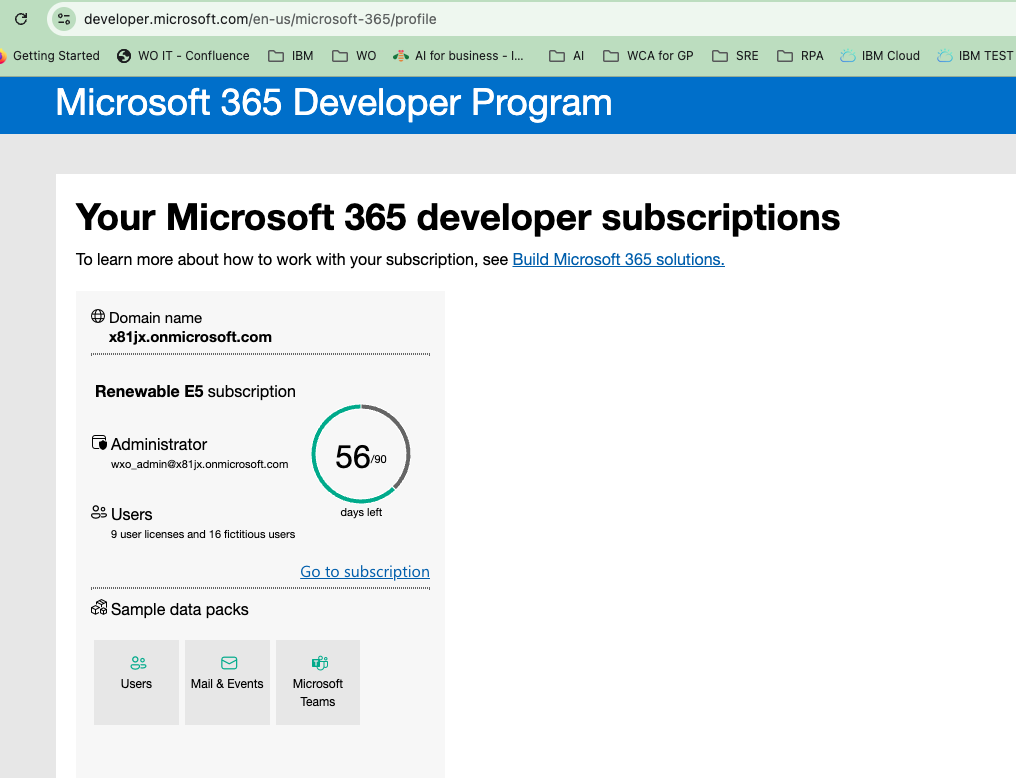
### client\_id



### client\_secret

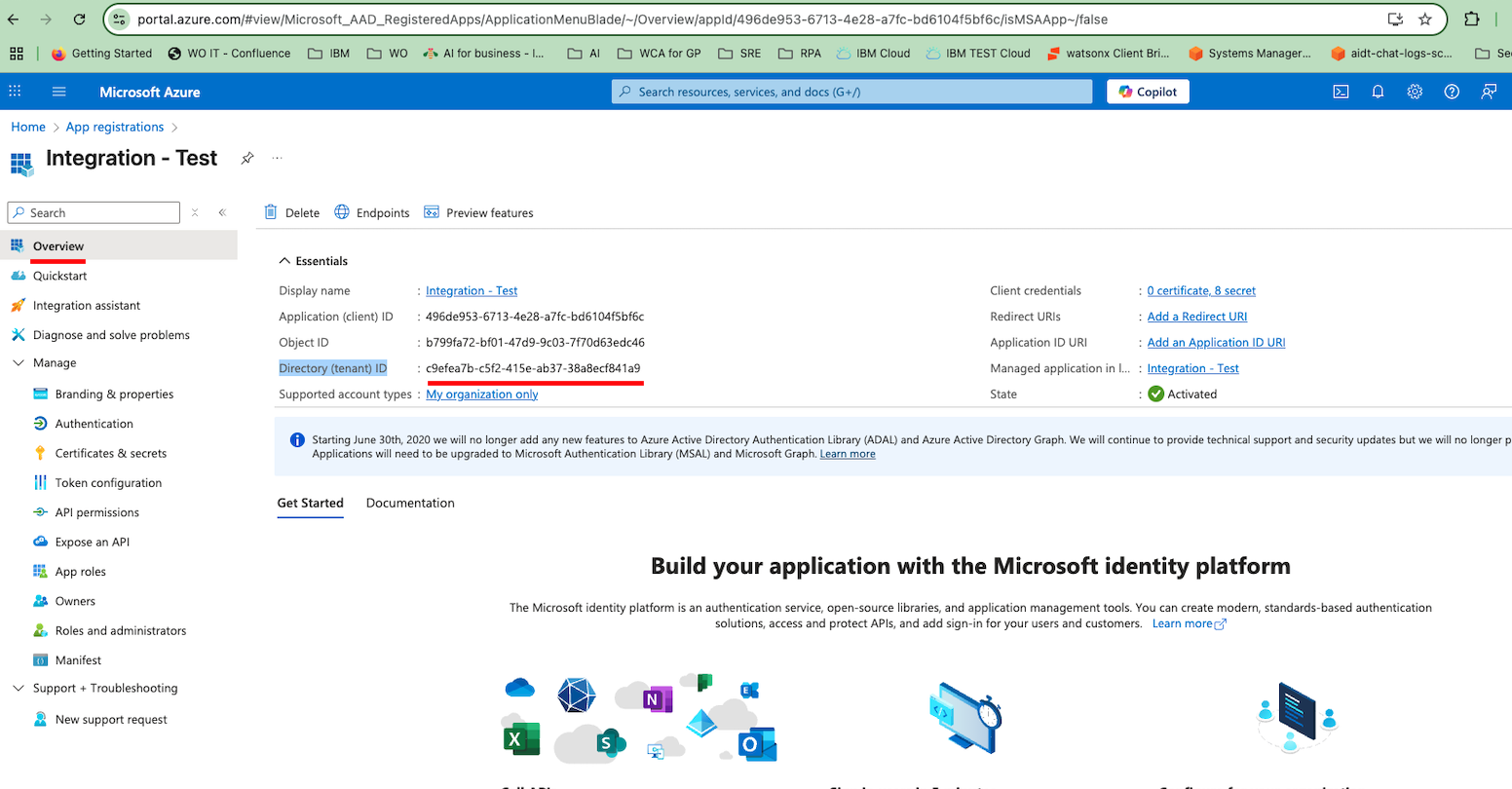
use value from clipboard at step 5

### Username



### Authority

https://login.microsoftonline.com/ + Directory (tenant) ID



### base\_url

<https://graph.microsoft.com>

Please follow https://www.ibm.com/docs/en/watsonx/watson-orchestrate/base?topic=agents-microsoft-outlook

## Examples

"client\_id": "496de953-6713-4e28-a7fc-bd6104f5bf6c",

"client\_secret": "bas8Q~x7qUIrMNUCja2EJV2X.dR7CSqdaye4aabm",

"username": "AdeleV@x81jx.onmicrosoft.com",

"password": "Adm!n1234567890",

"authority": <https://login.microsoftonline.com/c9efea7b-c5f2-415e-ab37-38a8ecf841a9>,

"base\_url": "[https://graph.microsoft.com](https://graph.microsoft.com/)"

"client\_id": "5bff183b-31a6-443c-86d7-0b67a0129bca",

"client\_secret": "r3X8Q~lEFaqBPQJKDaUy3jNmjZBpCRxyZ1EzbamY",

"username": "[testuser1@wxodomains.onmicrosoft.com](mailto:testuser1@wxodomains.onmicrosoft.com)",

"password": "---------------",

"authority": "<https://login.microsoftonline.com/wxodomains.onmicrosoft.com>",

"base\_url": "<https://graph.microsoft.com>"