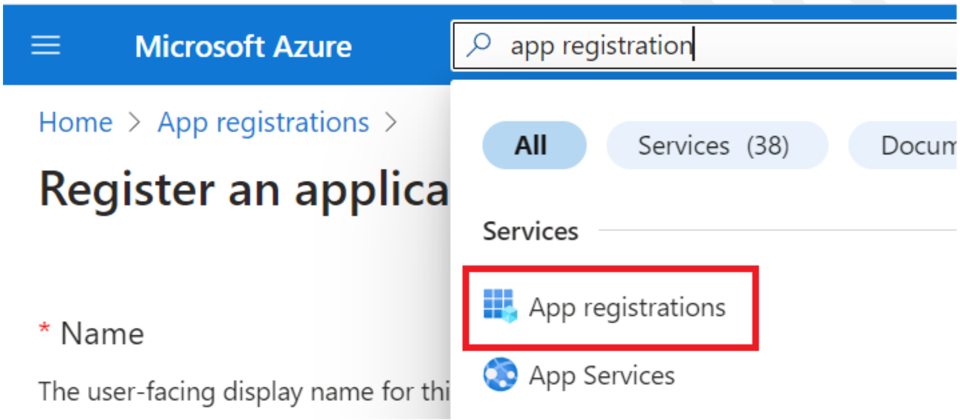
Get all Active Directory users in your organization

Go to app registrations in Azure

Create a new app



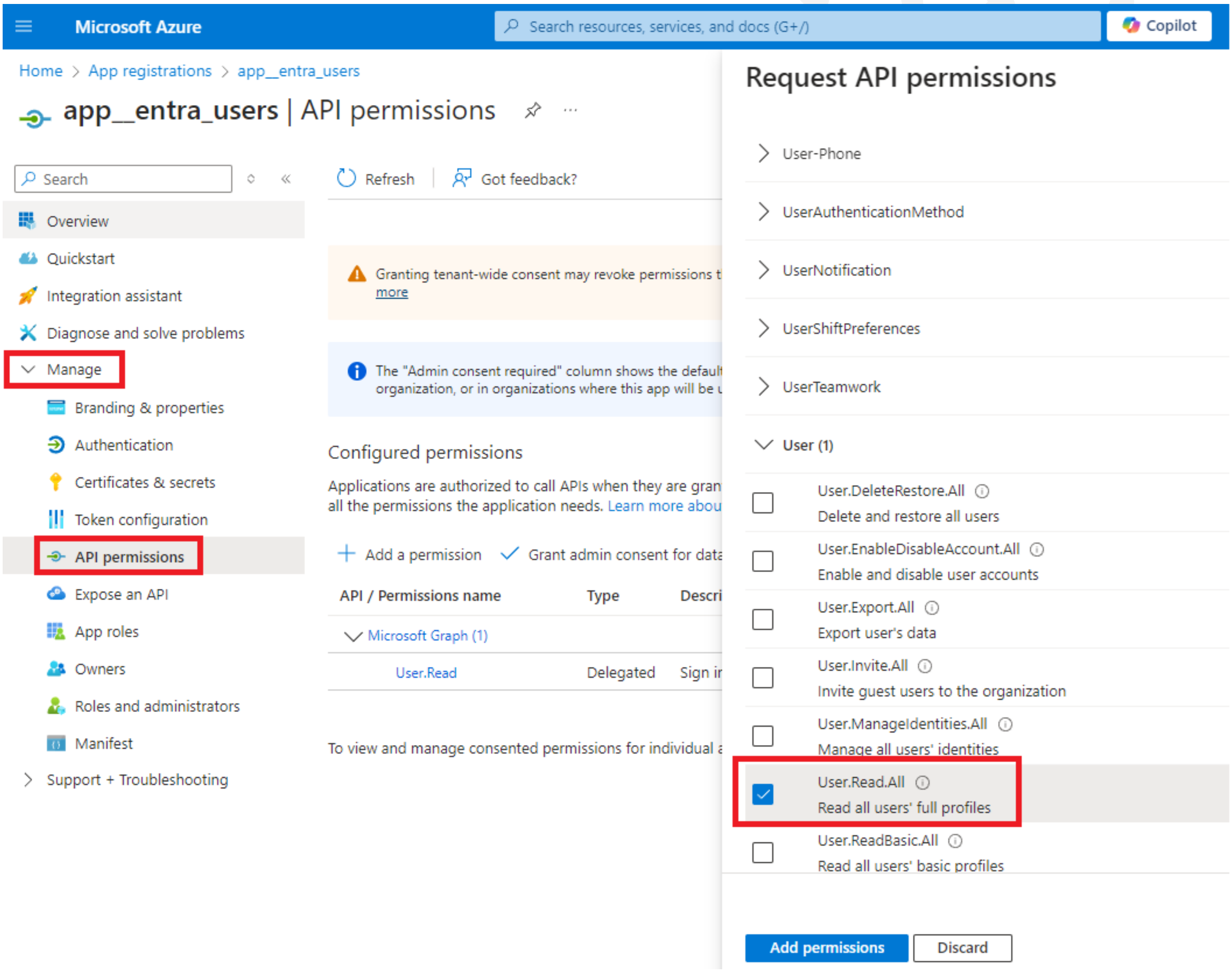
Go to tab “Manage”

Go to subtab “API permissions”

Click on “Add a permission”

Click on “Microsoft Graph”

Add the Application permission “User.Read.All”



Microsoft Azure

Search resources, services, and docs (G+/)

Copilot

Home > App registrations > app__entra_users

app__entra_users | API permissions

Search

- Overview
- Quickstart
- Integration assistant
- Diagnose and solve problems
- Manage
  - Branding & properties
  - Authentication
  - Certificates & secrets
  - Token configuration
  - API permissions
  - Expose an API
  - App roles
  - Owners
  - Roles and administrators
  - Manifest
- Support + Troubleshooting

Refresh | Got feedback?

Granting tenant-wide consent may revoke permissions t
more

The "Admin consent required" column shows the default
organization, or in organizations where this app will be u

Configured permissions

Applications are authorized to call APIs when they are gran
all the permissions the application needs. Learn more abou

+ Add a permission ✓ Grant admin consent for data

API / Permissions name	Type	Descri
Microsoft Graph (1)		
User.Read	Delegated	Sign ir

To view and manage consented permissions for individual a

Request API permissions

- User-Phone
- UserAuthenticationMethod
- UserNotification
- UserShiftPreferences
- UserTeamwork
- User (1)

□ User.DeleteRestore.All
Delete and restore all users

□ User.EnableDisableAccount.All
Enable and disable user accounts

□ User.Export.All
Export user's data

□ User.Invite.All
Invite guest users to the organization

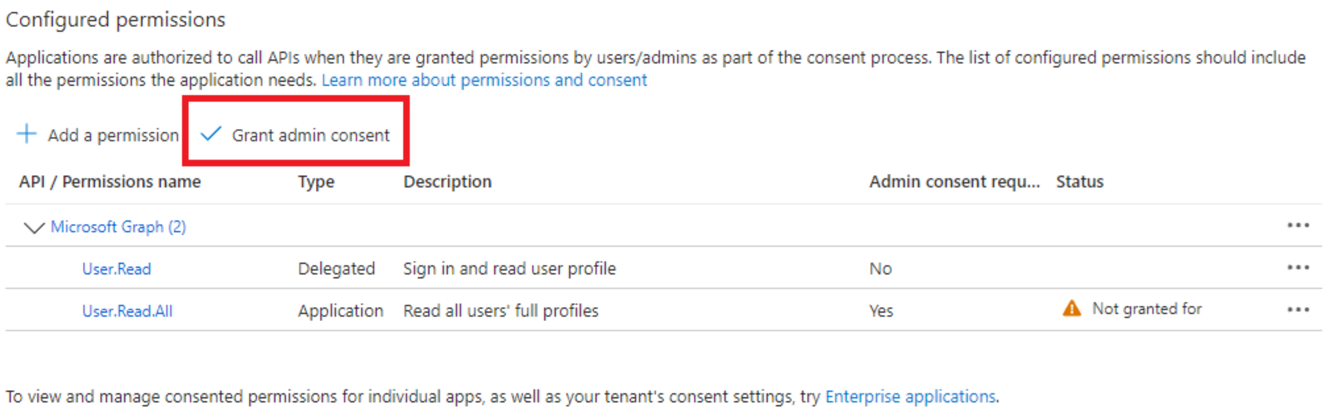
□ User.ManageIdentities.All
Manage all users' identities

☑ User.Read.All
Read all users' full profiles

□ User.ReadBasic.All
Read all users' basic profiles

Add permissions | Discard

Grant admin consent



Configured permissions

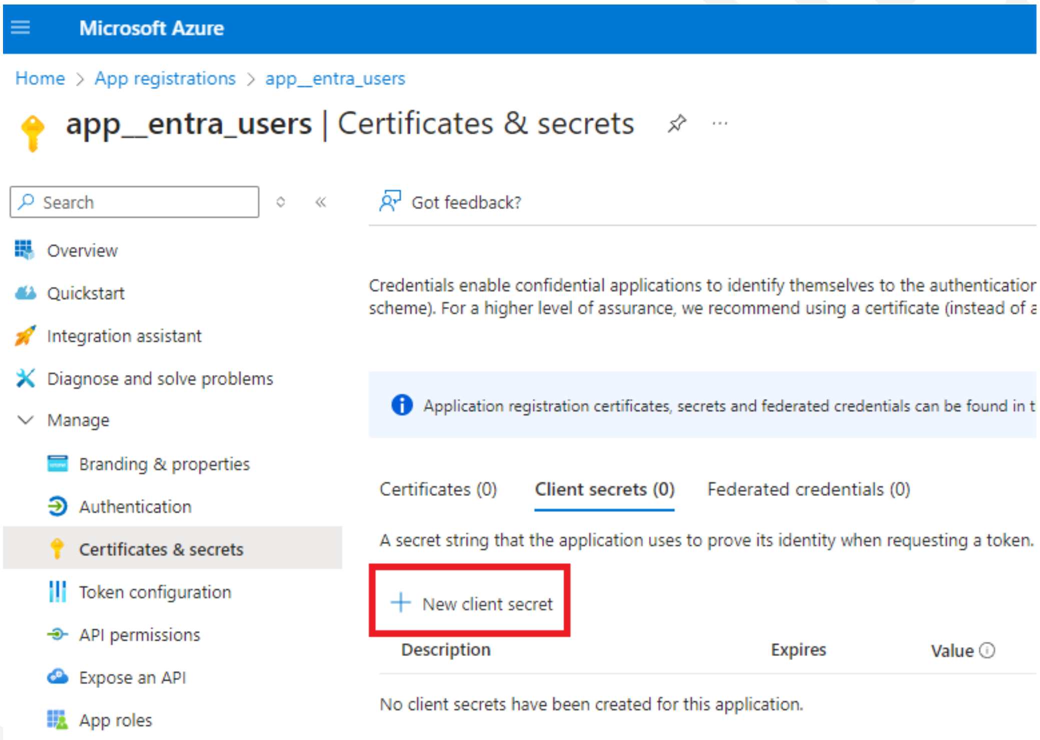
Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. Learn more about permissions and consent

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (2)				
User.Read	Delegated	Sign in and read user profile	No	
User.Read.All	Application	Read all users' full profiles	Yes	⚠ Not granted for

To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try Enterprise applications.

Go to Certificates and secrets

Click on New client secret



Credentials enable confidential applications to identify themselves to the authenticatior scheme). For a higher level of assurance, we recommend using a certificate (instead of a

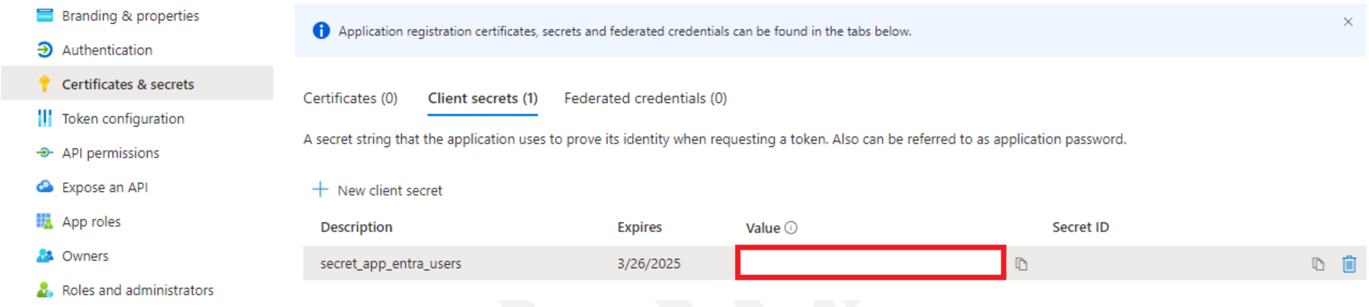
Application registration certificates, secrets and federated credentials can be found in t

A secret string that the application uses to prove its identity when requesting a token.

No client secrets have been created for this application.

Copy the value of the secret right after creation

Save it somewhere safe



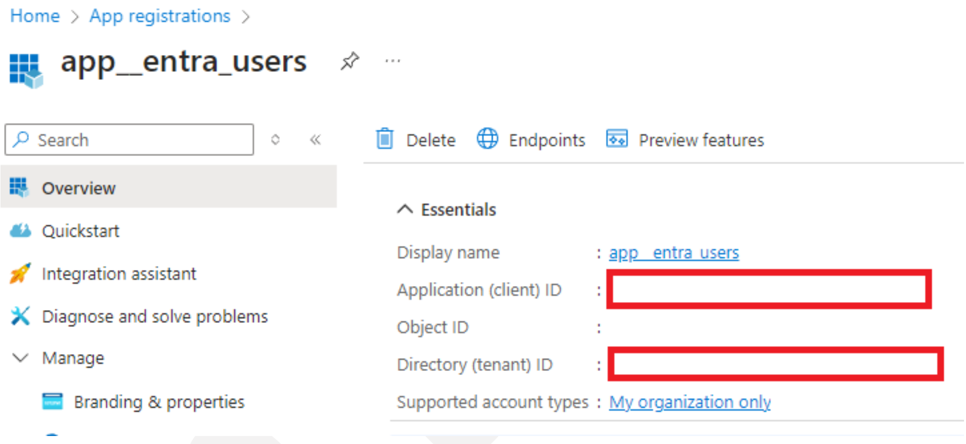
Application registration certificates, secrets and federated credentials can be found in the tabs below.

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

Description	Expires	Value ⓘ	Secret ID
secret_app_entra_users	3/26/2025		

Copy the Application (client) ID

Copy the Directory (tenant) ID



Display name : app__entra_users

Application (client) ID :

Object ID :

Directory (tenant) ID :

Supported account types : My organization only

For testing purposes create auth.py and create the following variables with the values that you copied earlier

Save auth.py in the same folder where the “API call” script (defined later in this document) is saved

```
tenant_id = "your tenant id"
client_id = "your client id"
client_secret = "your client secret"
```

Note: this is not a safe way to save authentication data so be sure to use a service that is designed to save this type of data like Azure Key Vault or AWS Key Management Service

Use the script below to pick up the AD users

(script below is not an image and can be copied)

```python
import requests
import json
import auth

# Get an access token from Microsoft Identity platform
tenant_id = auth.tenant_id
client_id = auth.client_id
client_secret = auth.client_secret
authority_url = f"https://login.microsoftonline.com/{tenant_id}/oauth2/v2.0/token"

body = {
    "grant_type": "client_credentials",
    "client_id": client_id,
    "client_secret": client_secret,
    "scope": "https://graph.microsoft.com/.default",
}

token_response = requests.post(authority_url, data=body)
token = token_response.json().get('access_token')

# Use the token to make an API request
headers = {
    "Authorization": f"Bearer {token}",
    "Content-Type": "application/json"
}

# API call to get all users
url = "https://graph.microsoft.com/v1.0/users"
response = requests.get(url, headers=headers)

# Print the result
users = response.json()
print(json.dumps(users, indent=4))
```