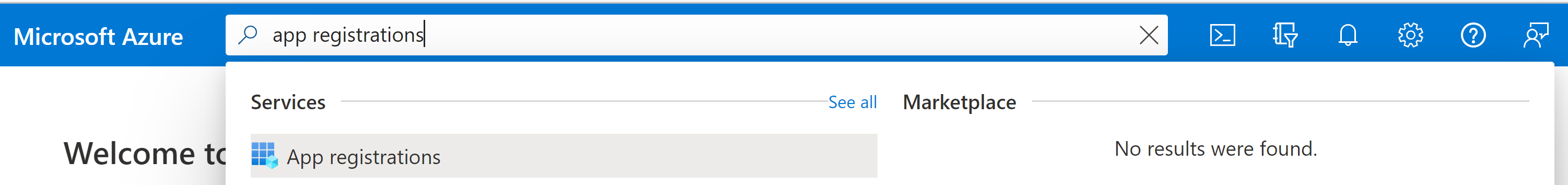
**Login to Microsoft Graph PowerShell SDK using app only authentication**

(For non-global admin users)

NOTE: You should have global admin rights to perform the following steps.

1. Login to ‘https://portal.azure.com’ using global admin credentials.
2. Go to app registrations. 
3. Select new registaration. Graphical user interface, application, chat or text message

   Description automatically generated
4. Set the name and supported account type as shown below: Graphical user interface, text, application, email

   Description automatically generated
5. Leave Redirect URI blank and click on Register.

Graphical user interface, text, application, email

Description automatically generated

1. Under Certificates & secrets, you have to upload certificate. You can either upload an existing X.509 certificate or create a new one and then upload it. Graphical user interface, application, table

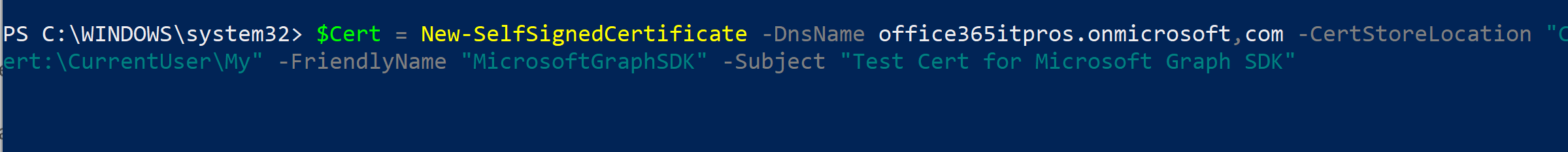
   Description automatically generated

Creating new X.509 certificate using PowerShell:

1. Run the following command:

$Cert = New-SelfSignedCertificate -CertStoreLocation "Cert:\CurrentUser\My" -FriendlyName "MicrosoftGraphSDK" -Subject "Test Cert for Microsoft Graph SDK"

Get-ChildItem "Cert:\CurrentUser\My\$($Cert.thumbprint)"



Graphical user interface, text, application

Description automatically generated

1. After creating the certificate, we export it to a .cer file.

Run the following command to export the .cer file to the specified FilePath.

Get-ChildItem "Cert:\CurrentUser\My\$($Cert.thumbprint)" | Export-Certificate -FilePath C:\WINDOWS\system32\MicrosoftGraphSDK.cer Graphical user interface, text

Description automatically generated

1. Upload the certificate created.

Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

1. Store the thumbprint of the certificate. Text

   Description automatically generated
2. Under API permissions, click on Add a permission

Graphical user interface, text, application, email

Description automatically generated

1. Click on Microsoft Graph under Microsoft APIs Graphical user interface, application, email

   Description automatically generated
2. Click on Application Permissions. Graphical user interface, application

   Description automatically generated
3. Add eDiscovery.ReadWrite.All permisssionGraphical user interface, text, application, Teams

   Description automatically generated
4. Grant Admin Consent for Contoso Graphical user interface, text, application, email

   Description automatically generated
5. Under overview tab, you can find client id and tenant id.Graphical user interface, application

   Description automatically generated
6. Use client id, tenant id and certificate thumbprint (from step 10) to login to the tool/mggraph. Share these values with the eDiscovery Admin and other users who want to use the tool.
7. Run this command to connect to the mggraph.

Connect-MgGraph -ClientID <ClientID> -TenantId < TenantId > -CertificateThumbprint < CertificateThumbprint >

1. Login to eDiscovery Shift App using app credentials as shown below: Text

   Description automatically generated with medium confidence