Access SPO using Sites.Selected

Contents

Overview

SPO REST API introduced Sites.Selected permission which allows an application to access specific site collection via SPO REST API. This approach generally involves the following high level steps:

- Create Azure AD Application with “Sites.Selected” permissions and a certificate as a secret.
- Create Azure AD application to grant above Azure AD Application to a site collection via MS Graph API

When developers access the SPO via App-only approach, SPO requires to use certificate as credential instead of regular secret. The administrators also need to provide a certificate when they register an Azure AD Application secret. The certificate can be part of enterprise CA management.

Configuration

Create self-sign certificate

This is for demo purpose. For production, please create a certificate from your enterprise Certificate Authority.

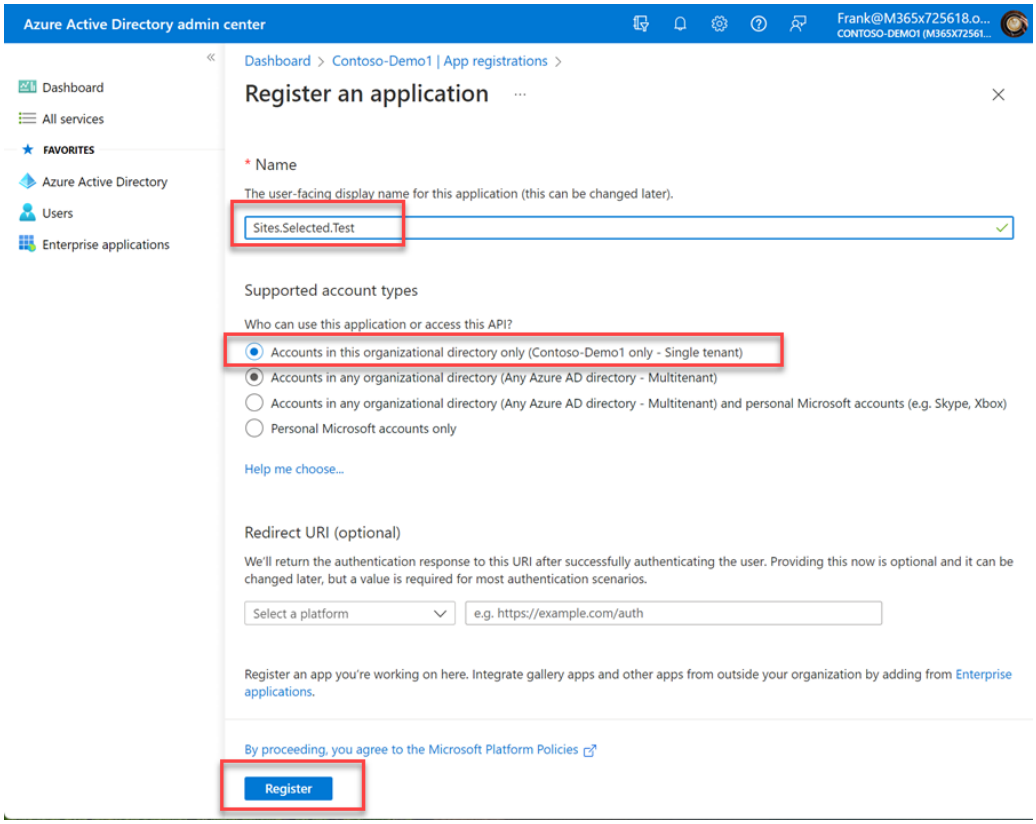
Please check out Step 3: Generate a self-signed certificate to create certificate. You should have the following certificate created:

- .pfx: the certificate with private key
- .cer: the certificate which is exported from .pfx without private key
- Certificate password: the password used for certificate.

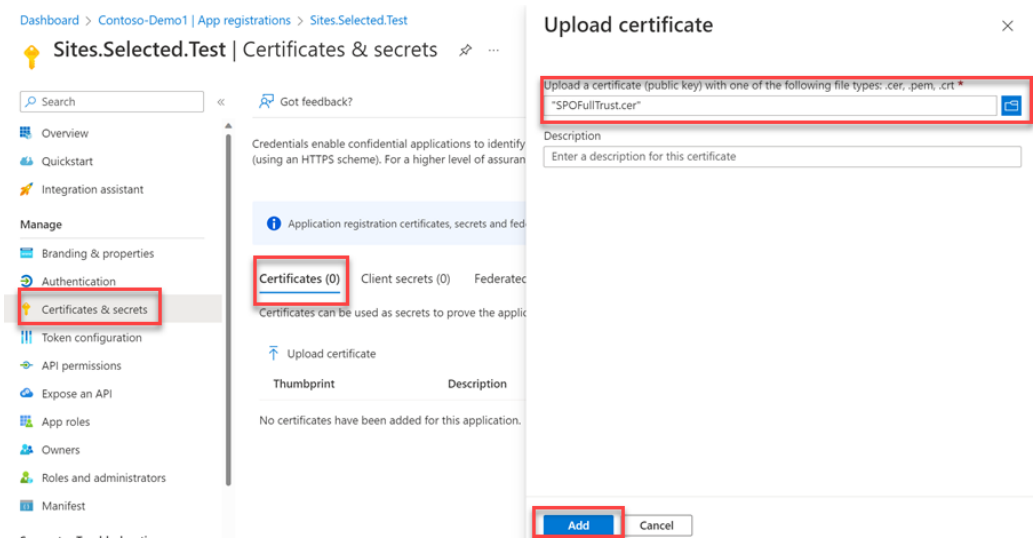
Azure AD Application with “Sites.Selected” permission

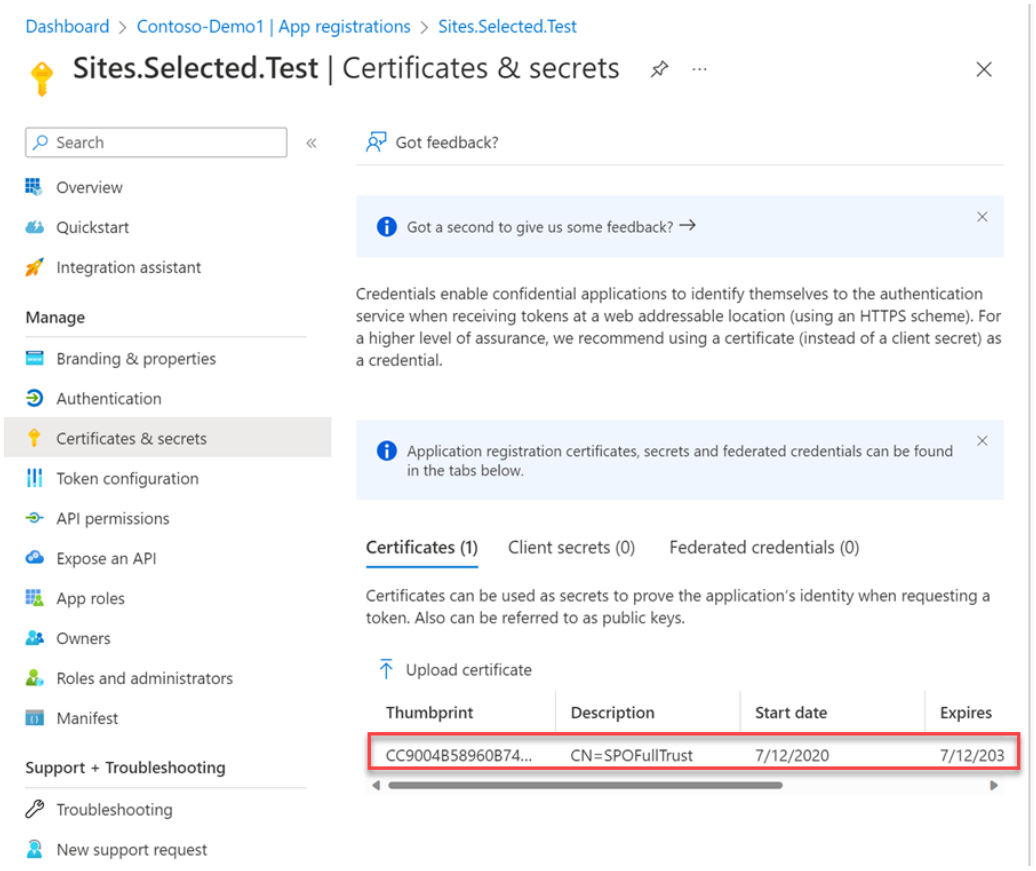
It’s required to create an Azure AD Application to use Sites.Selected permission. Please refer to the below steps:

1. Go to Azure AD admin center via https://aad.portal.azure.com
2. Go to “Azure Active Directory” -> “App Registration” to create a Azure AD application.
3. Click “New registration”, provide the following information
    a. Name: The Azure AD application name
    b. Who can use this application or access this API: select “Accounts in this organization directory only” if you want to you application is just for your tenant.
    c. Click “Register” button to create the Azure AD Application

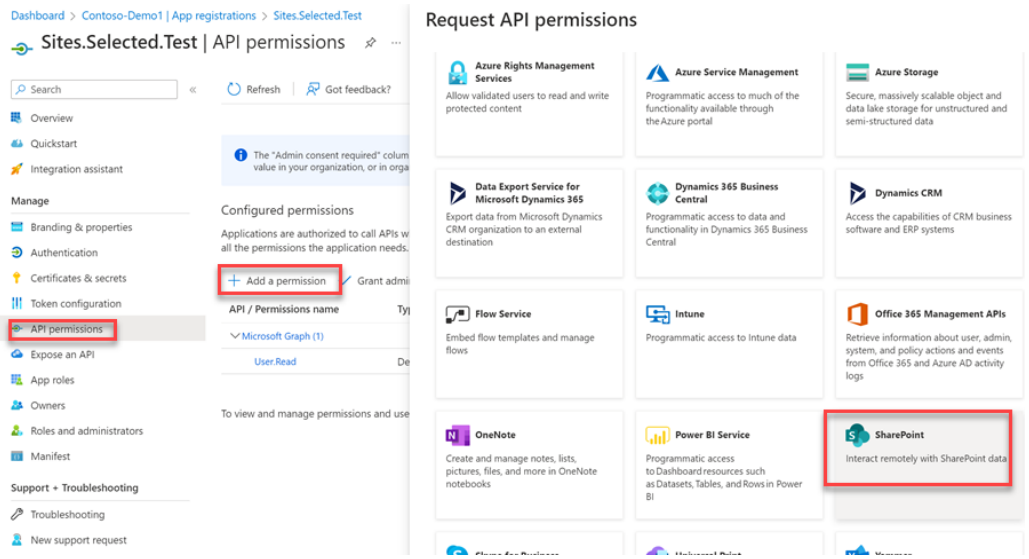


4. Once the Azure AD application is created, click “Certificates & secrets” to update certificate.
    a. Click “Certificates” tab
    b. Click “Upload certificate” button to bring up the “Upload certificates” pane
    c. Select .cer file which you generated from previous steps.
    d. Click “Add” button to upload.

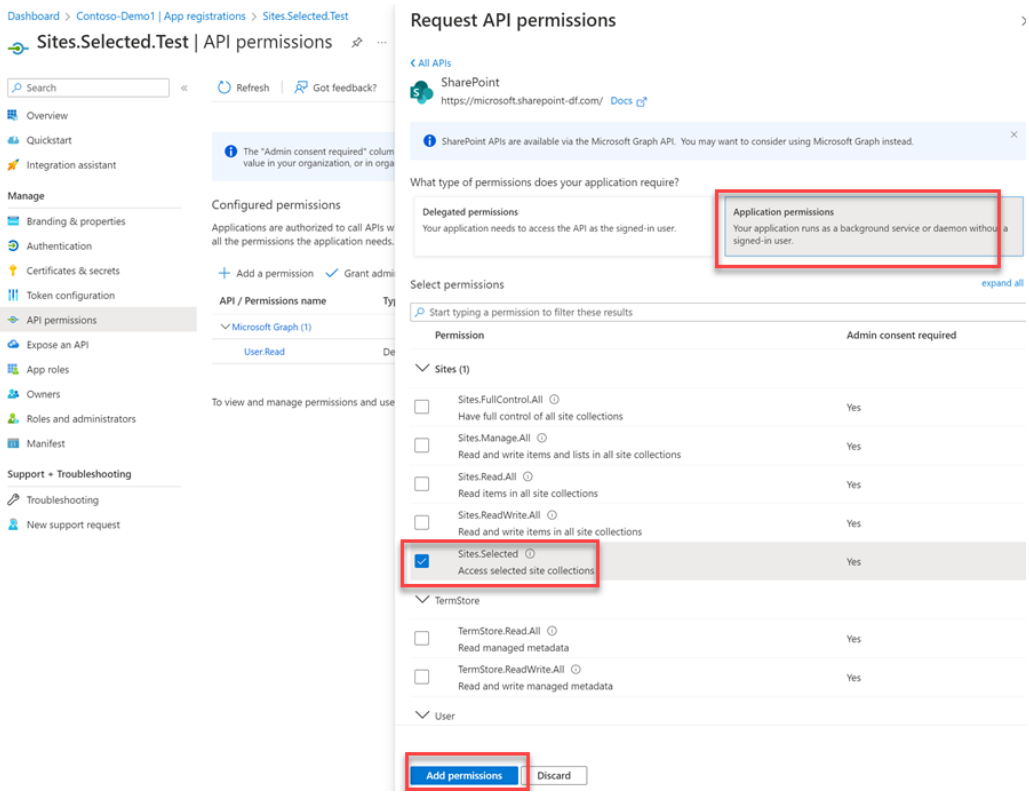


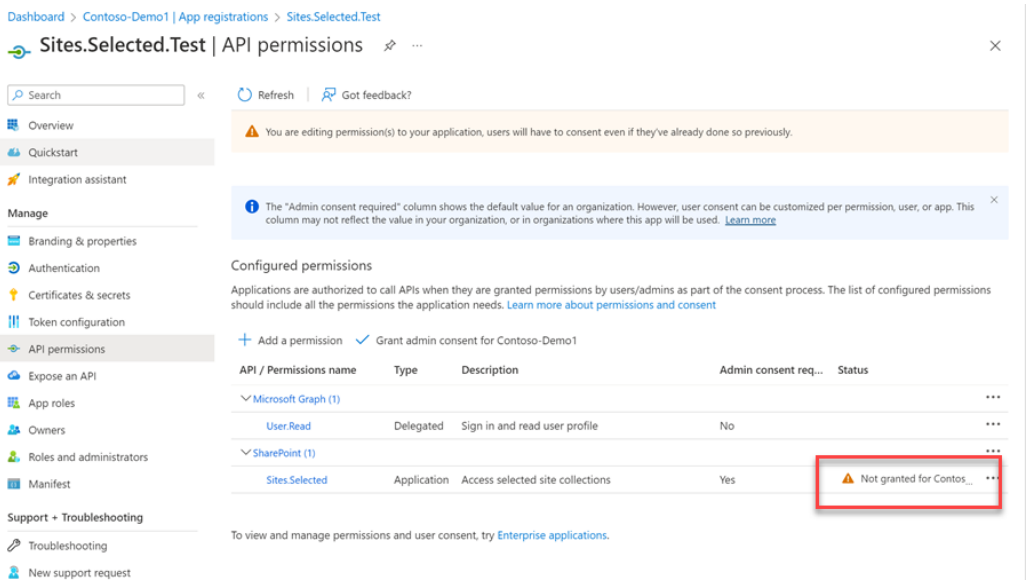


5. Click “API permissions” tab to configure the SPO REST API permissions
    a. Click “Add permission” button to bring up “Request API permissions” pane
    b. Select “SharePoint”

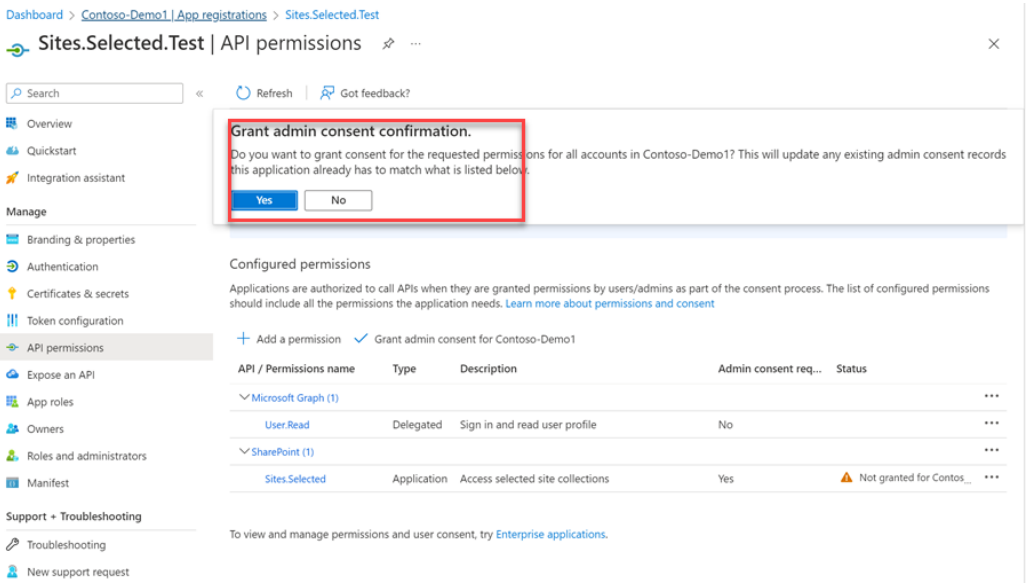


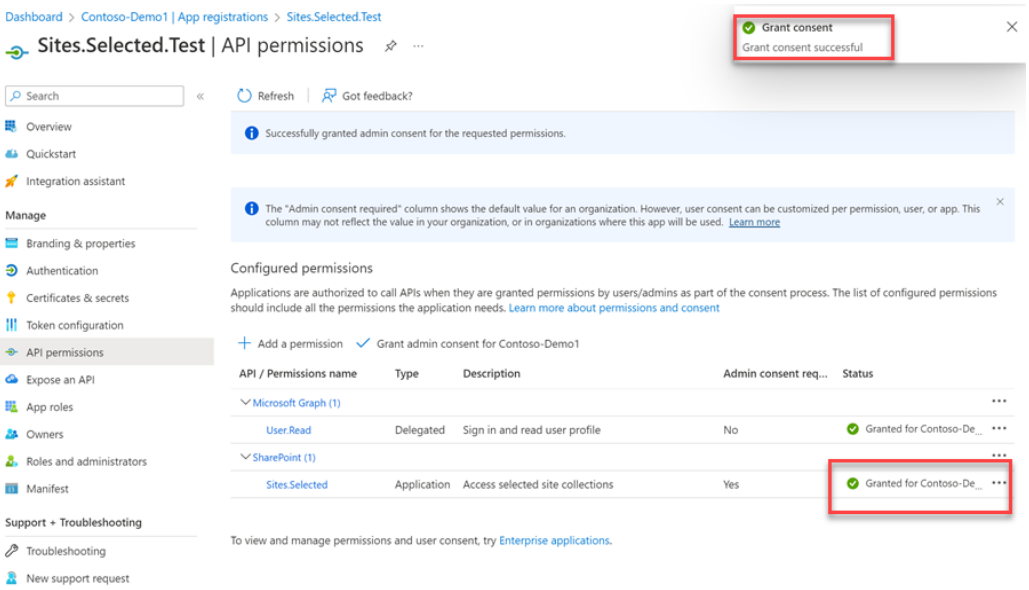
c. Select “Application permissions”
d. Select “Sites.Selected” permission under “Site”.
e. Click “Add permission” button





f. Once you added “Sites.Selected” permission. You need to perform administrator consent to consent the permission. Click “Grant admin consent for [tenant-name]” button.



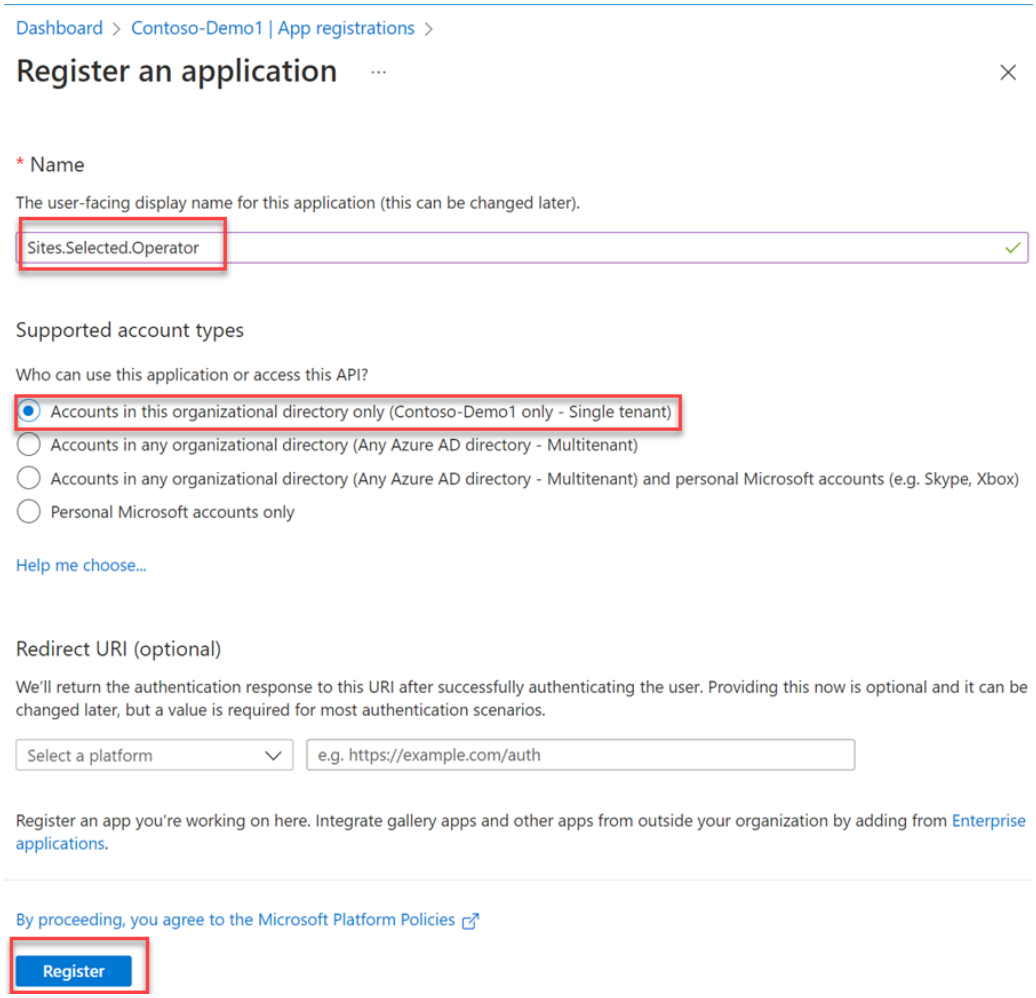


g. You can use the same process to add Sites.Selected permission from MS Graph API.

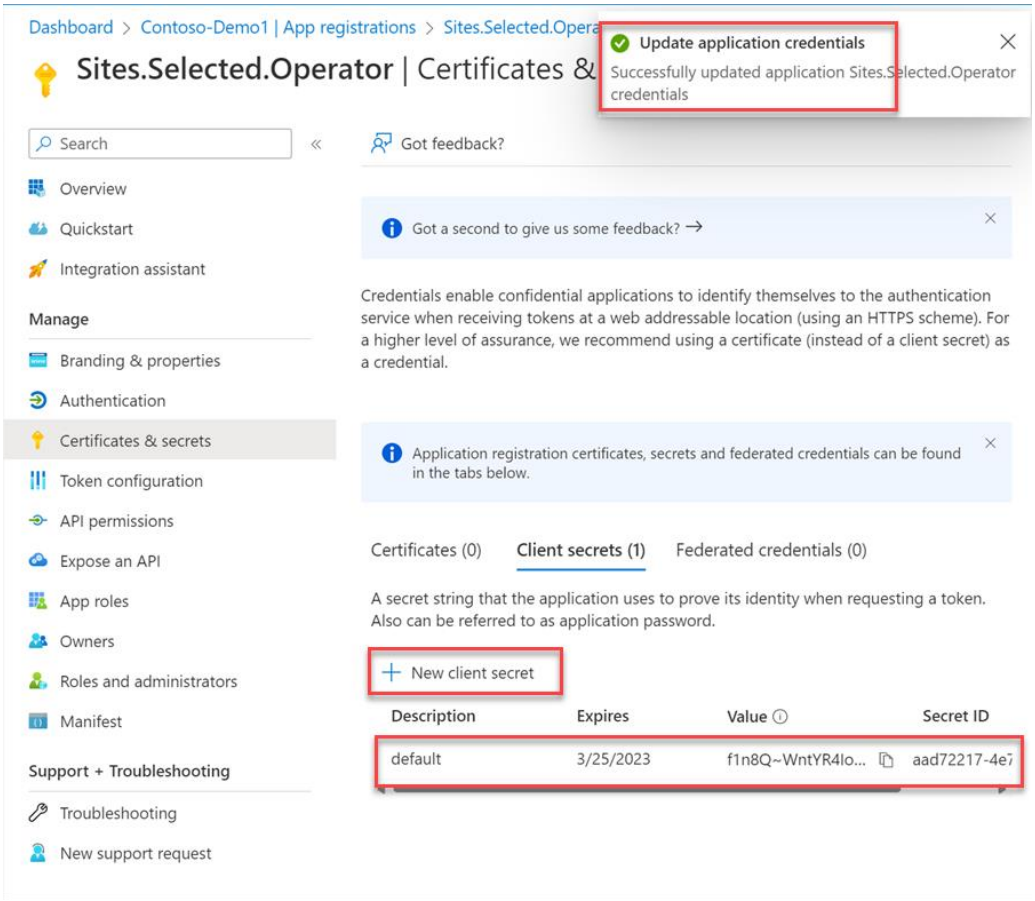
Azure AD Application which can grant the site permissions.

Once we created Azure AD application with “Sites.Selected” permission, we need to leverage another Azure AD application grant above Azure AD App to specific site collections.

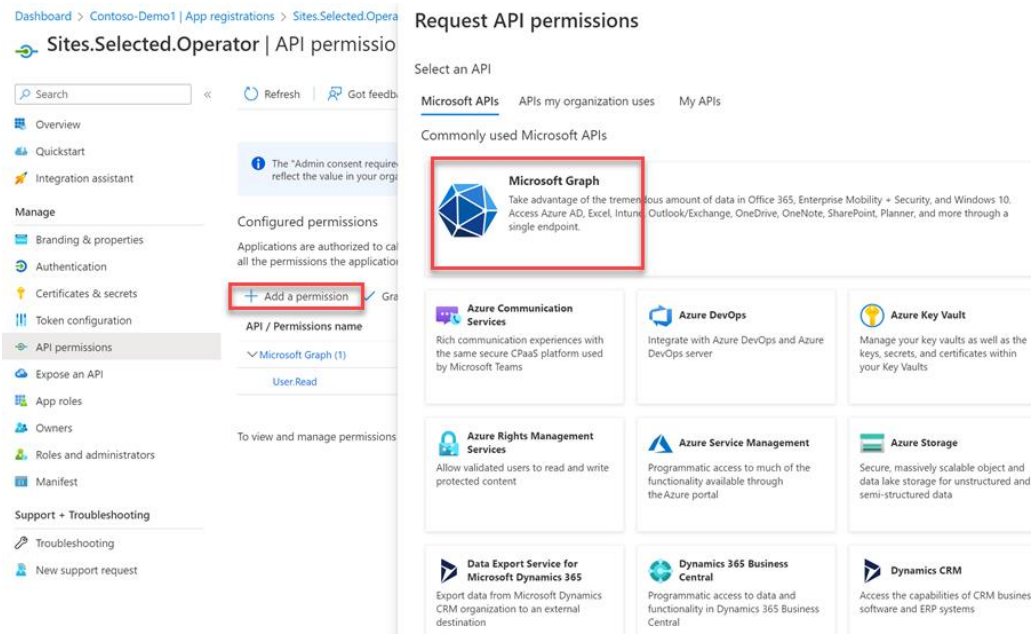
1. Go to Azure AD admin center via https://aad.portal.azure.com
2. Go to “Azure Active Directory” -> “App Registration” to create a Azure AD application.
3. Click “New registration”, provide the following information
    a. Name: the Azure AD application name
    b. Who can use this application or access this API: select “Accounts in this organization directory only” if you want to you application is just for your tenant.
    c. Click “Register” button to create the Azure AD Application



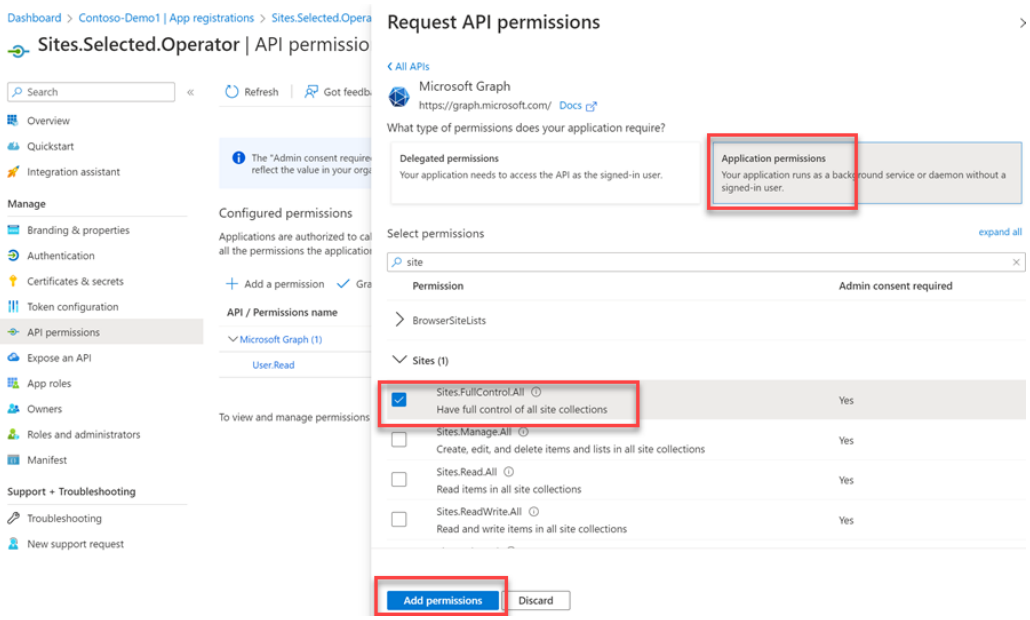
4. Once the Azure AD application is created, click “Certificates & secrets” to update certificate.
    a. Click “Client secrets” tab
    b. Click “New client secret” button to generate a secret. By default, the secret with 6 months period will be created.

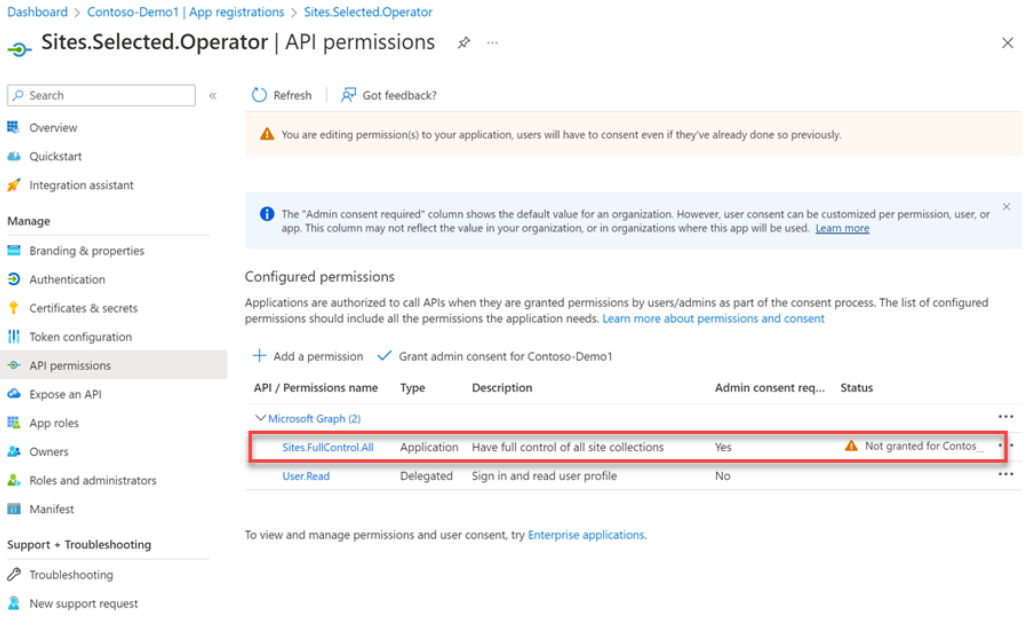


5. Click “API permissions” tab to configure the SPO REST API permissions
    a. Click “Add permission” button to bring up “Request API permissions” pane
    b. Select “Microsoft Graph”

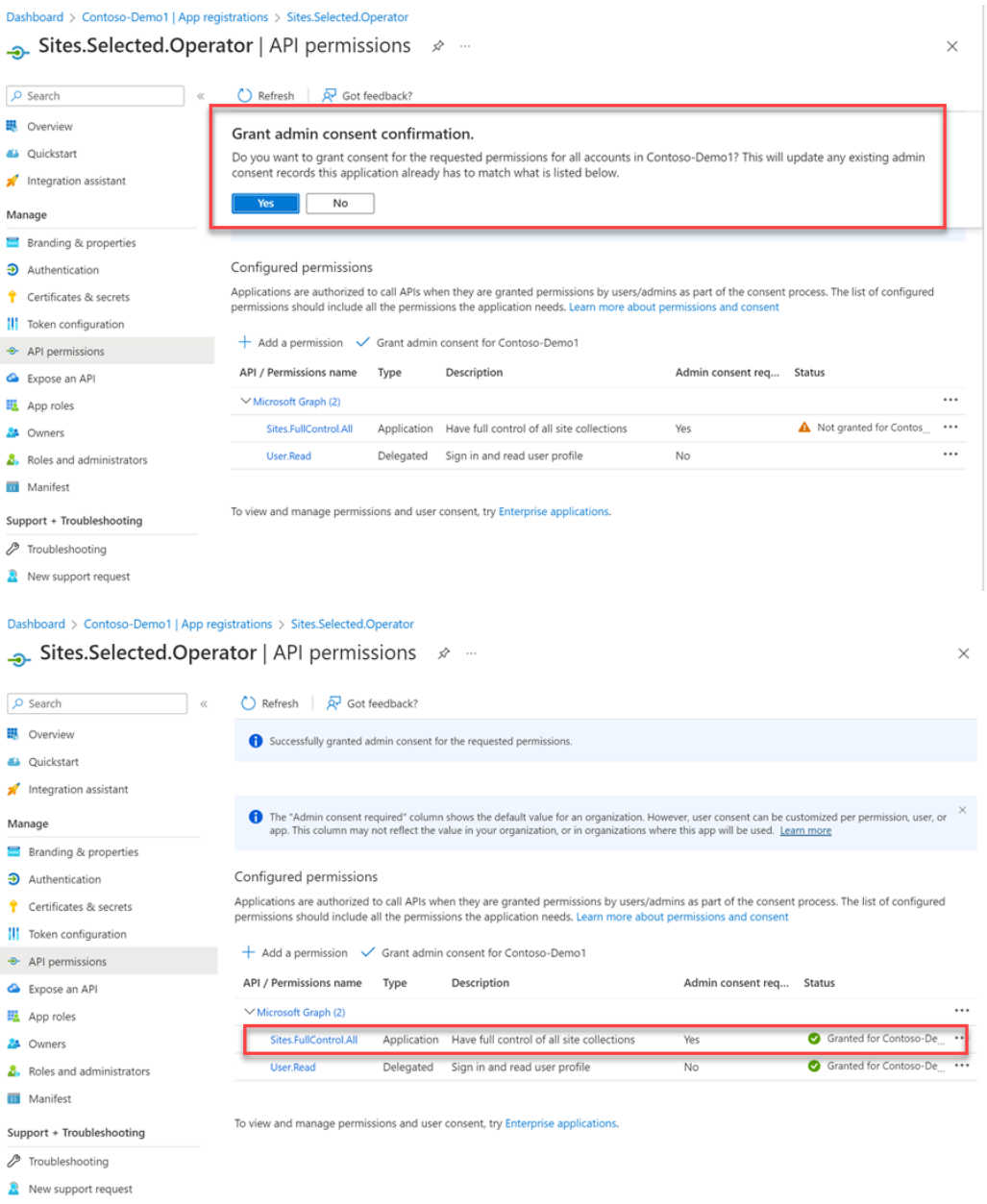


c. Select “Application permissions”
d. Select “Sites.FullControl.All” permission under “Site”.
e. Click “Add permission” button





f. Once you added “Sites.FullControl.All” permission. You need to perform administrator consent to consent the permission. Click “Grant admin consent for [tenant-name]” button.



Grant Azure AD application to site collection via PnP PowerShell

You can use [Grant-PnPAzureADAppSitePermission] cmdlet from PnP PowerShell module to grant the permissions to site collection.

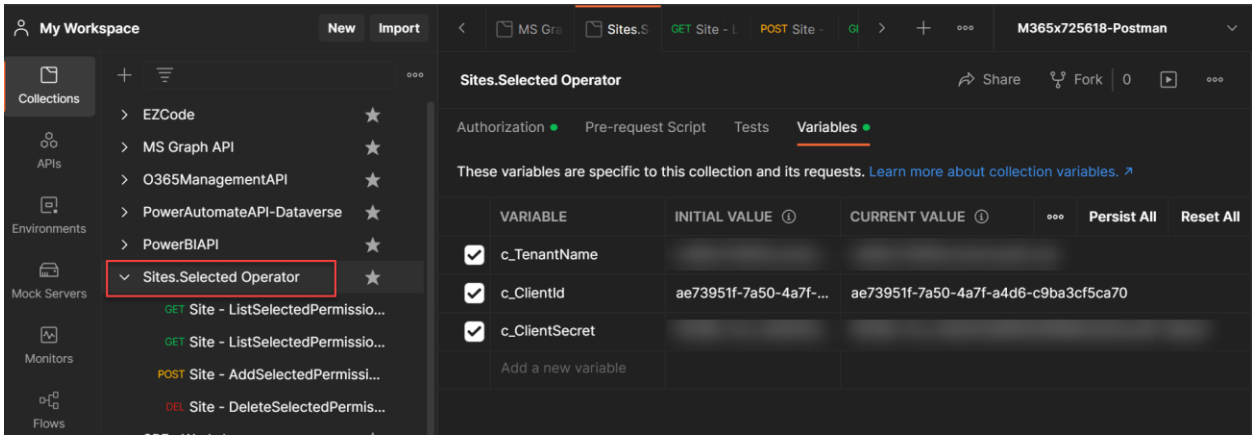
```
$siteUrl = "https://m365x725618.sharepoint.com/sites/FrankCommunication1"

# use below cmdlet if you have pfx certificate file
Connect-PnPOnline -Url $siteUrl `
   -ClientId [pnp-aad-app-clientid] `
   -Tenant [aad-tenant-name]`
   -CertificatePath "[certificate-path].pfx" `
```

```
   -CertificatePassword (ConvertTo-SecureString -String "[password]" -AsPlainText -Force)

# use below cmdlet if you have pfx installed in your local certificate store local machine->Personal store->
"[PnPPowerShell-certificate]"
Connect-PnPOnline -Url $siteUrl `
   -ClientId [pnp-aad-app-clientid] `
   -Tenant [aad-tenant-name] `
   -Thumbprint 467b1f87493fffb87e711a4e2a92bdd9ce9472a7 `

# appid: the aad app id which you configured site.selected permission
# displayName: this can be same as your aad app display name.
# permissions: it can be read or write
Grant-PnPAzureADAppSitePermission -AppId "aa37b89e-75a7-47e3-bdb6-b763851c61b6" -DisplayName
"Site.Selected.Test" -Permissions Read
```

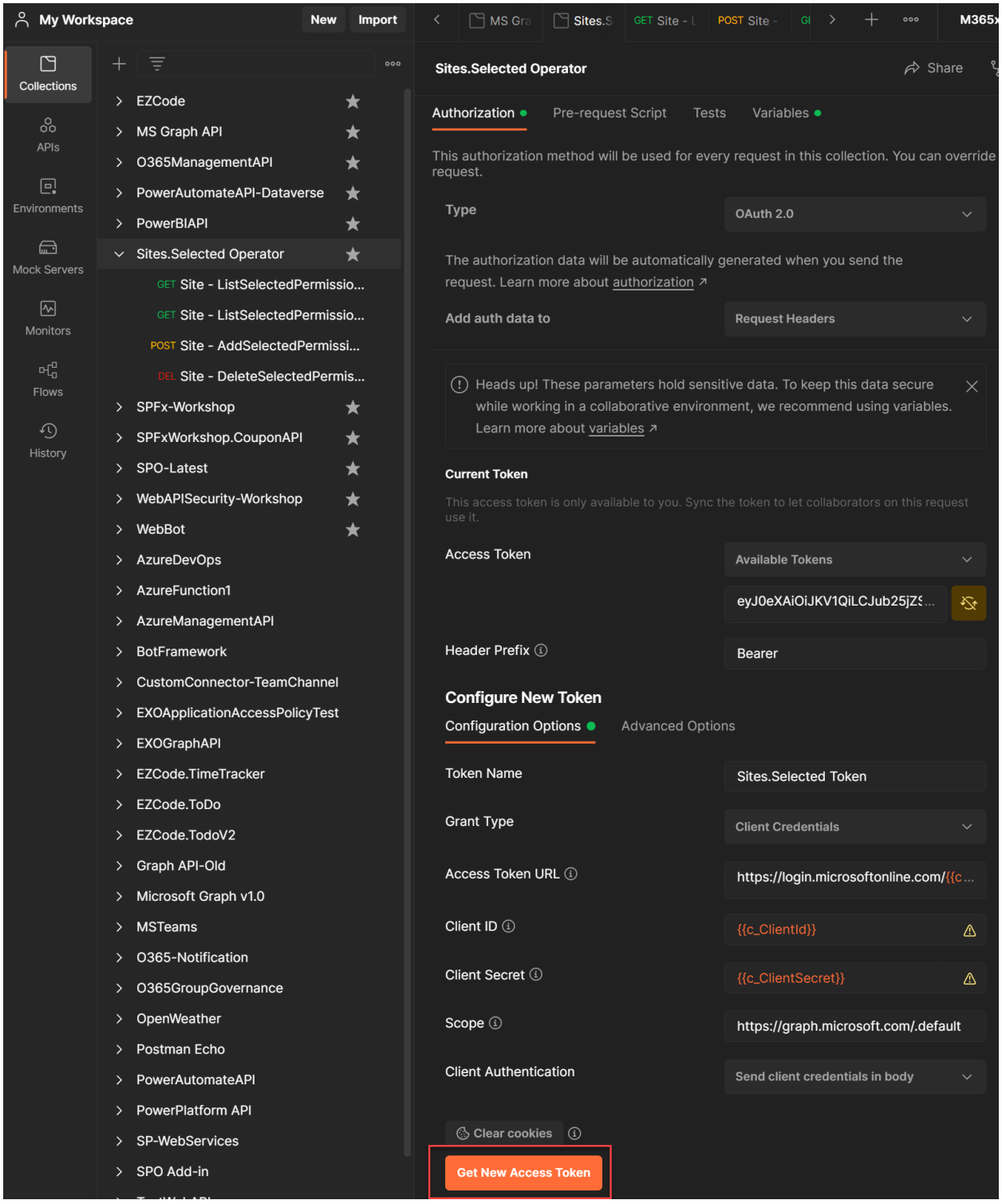
Grant Azure AD application to site collection via MS Graph API

Once we have two Azure AD Applications created, we can grant Azure AD App permissions to specific site collections via MS Graph API Create permission. The follow steps list details:

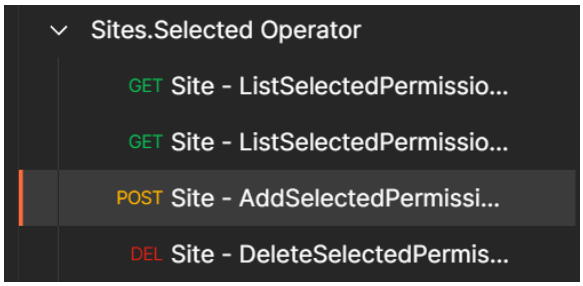
1. Download Postman collection json from SPOSitesSelected
2. Click “File” -> “Import” menu to import json file which you download from above step.
3. Click “…” right beside the collection name and click “Edit” context menu to bring up the collection property window. Select “Variables” tab and configure the collection variables as below:
    - c_TenantName: the tenant name
    - c_ClientId: the Azure AD application ID which we created from Application which can grant the site permissions.
    - c_ClientSecret: the Azure AD Application secret we created from Application which can grant the site permissions.



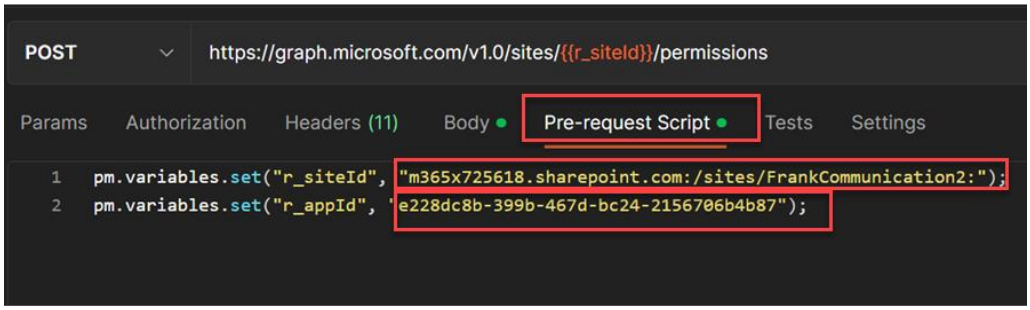
4. Select “Authorization” tab, then click “Get New Access Token” to generate the access token



5. Select “Site - AddSelectedPermissions” request. The request detail information is shown up.

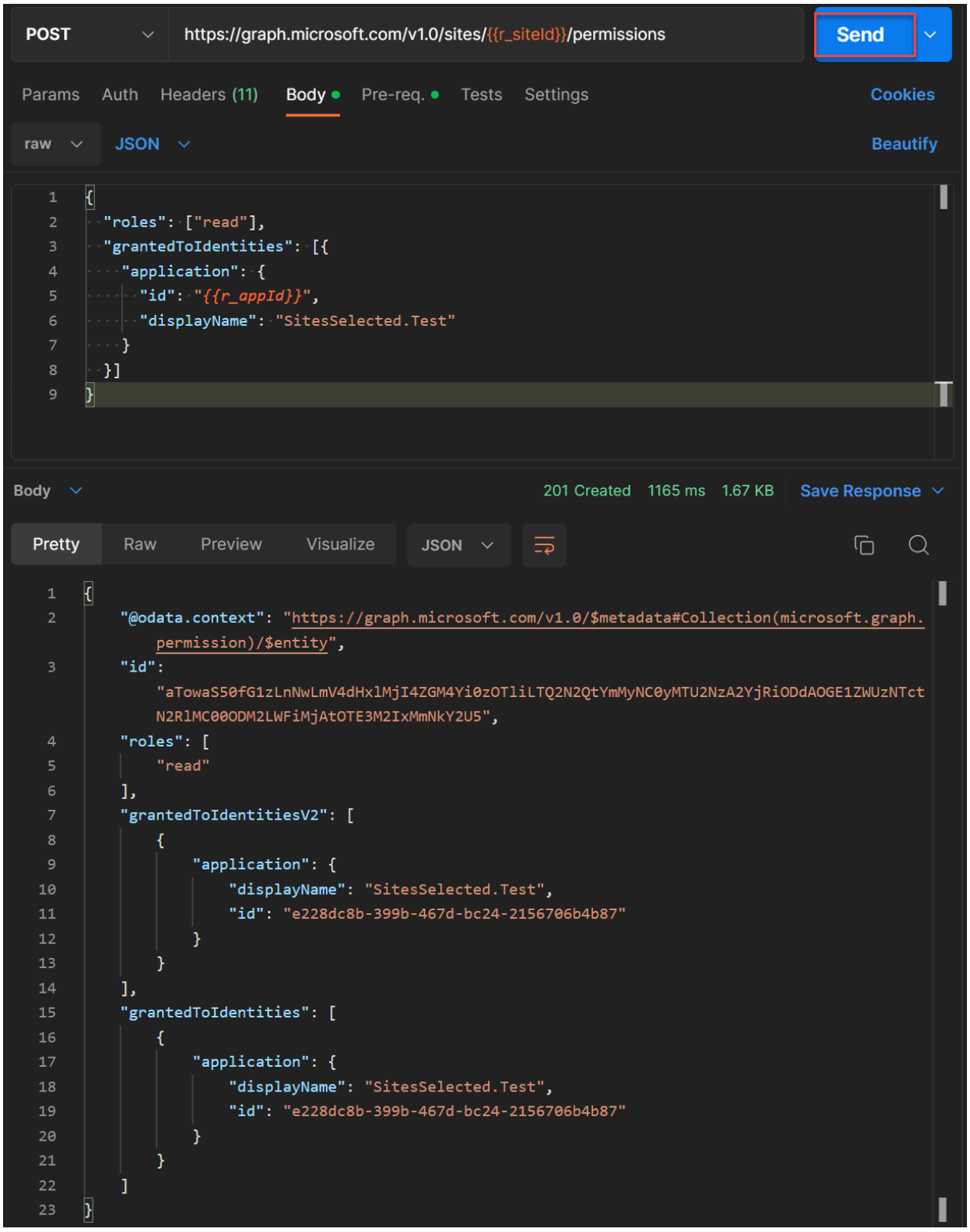


6. Click “Pre-request Script” tab and update the follow variables:
    - “r_siteId”: this is site id which can be “[spo-tenant-name]:/[site-collection-relative-url]”
    - “r_appId”: the Azure AD Application Id which were created from Azure AD Application with “Sites.Selected” permission step



7. Click “Body” tab and update “roles” to “read”, “write” or “read” and “write”

8. Click “Send” button to send the request. You should see the below result indicating that the permission has been granted to Azure AD Application.



Testing

Once you granted the permission to the Azure AD application, you can follow the below steps to check.

1. Follow Installing PnP PowerShell to install PnP PowerShell
2. Follow Authentication to configure your PnP PowerShell authentication.
3. Install .pfx file which we generated from Create self-sign certificate into your Certificate Store and record the certificate Thumbprint.
4. Call below PS cmdlet to test the Azure AD application which you created from Azure AD Application with "Sites.Selected" permission step

```
# site collection Url
$siteUrl = "https://m365x725618.sharepoint.com/sites/FrankCommunication2"
# Connect to SPO with Azure AD Application Id
Connect-PnPOnline -Url $siteUrl `
   -ClientId [aad-app-id]`
   -Tenant [tenant-id]`
   -Thumbprint [certificate-thumbprint]

# Get Web info
Get-PnPWeb
```