

Access SPO using Sites.Selected

Contents

Access SPO using Sites.Selected.....	1
Overview	1
Configuration	1
Create self-sign certificate.....	1
Azure AD Application with “Sites.Selected” permission	1
Azure AD Application which can grant the site permissions.....	6
Grant Azure AD application to site collection via PnP PowerShell.....	10
Grant Azure AD application to site collection via MS Graph API	11
Testing	14

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

Azure Active Directory admin center

Dashboard > Contoso-Demo1 | App registrations >

Register an application

* Name

The user-facing display name for this application (this can be changed later).

Sites.Selected.Test

Supported account types

Who can use this application or access this API?

☒ Accounts in this organizational directory only (Contoso-Demo1 only - Single tenant)

☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant)

☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

☐ Personal Microsoft accounts only

[Help me choose...](#)

Redirect URI (optional)

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.

Select a platform

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from [Enterprise applications](#).

By proceeding, you agree to the [Microsoft Platform Policies](#)

Register

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.

Dashboard > Contoso-Demo1 | App registrations > Sites.Selected.Test

Sites.Selected.Test | Certificates & secrets

Search

Got feedback?

Overview
Quickstart
Integration assistant

Manage

- Branding & properties
- Authentication
- Certificates & secrets**
- Token configuration
- API permissions
- Expose an API
- App roles
- Owners
- Roles and administrators
- Manifest

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 (0) Federated credentials (0)

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

Upload certificate

Thumbprint	Description
No certificates have been added for this application.	

Upload certificate (public key) with one of the following file types: .cer, .pem, .crt *

~SPOFullTrust.cer

Description

Enter a description for this certificate

Add Cancel

Dashboard > Contoso-Demo1 | App registrations > Sites.Selected.Test

Sites.Selected.Test | Certificates & secrets

Search

Got feedback?

Overview
Quickstart
Integration assistant

Manage

- Branding & properties
- Authentication
- Certificates & secrets**
- Token configuration
- API permissions
- Expose an API
- App roles
- Owners
- Roles and administrators
- Manifest

Support + Troubleshooting

- Troubleshooting
- New support request

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.

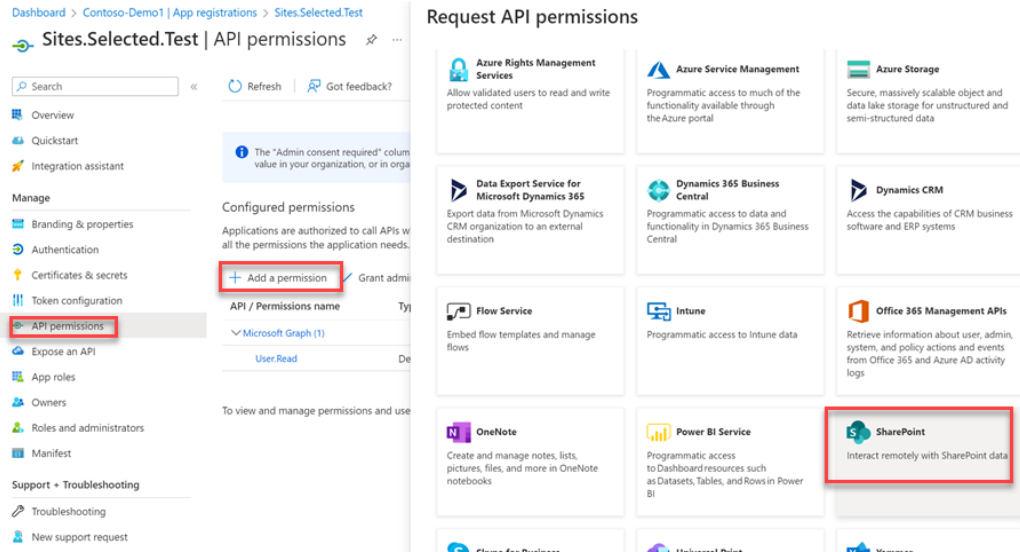
Certificates (1) Client secrets (0) Federated credentials (0)

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

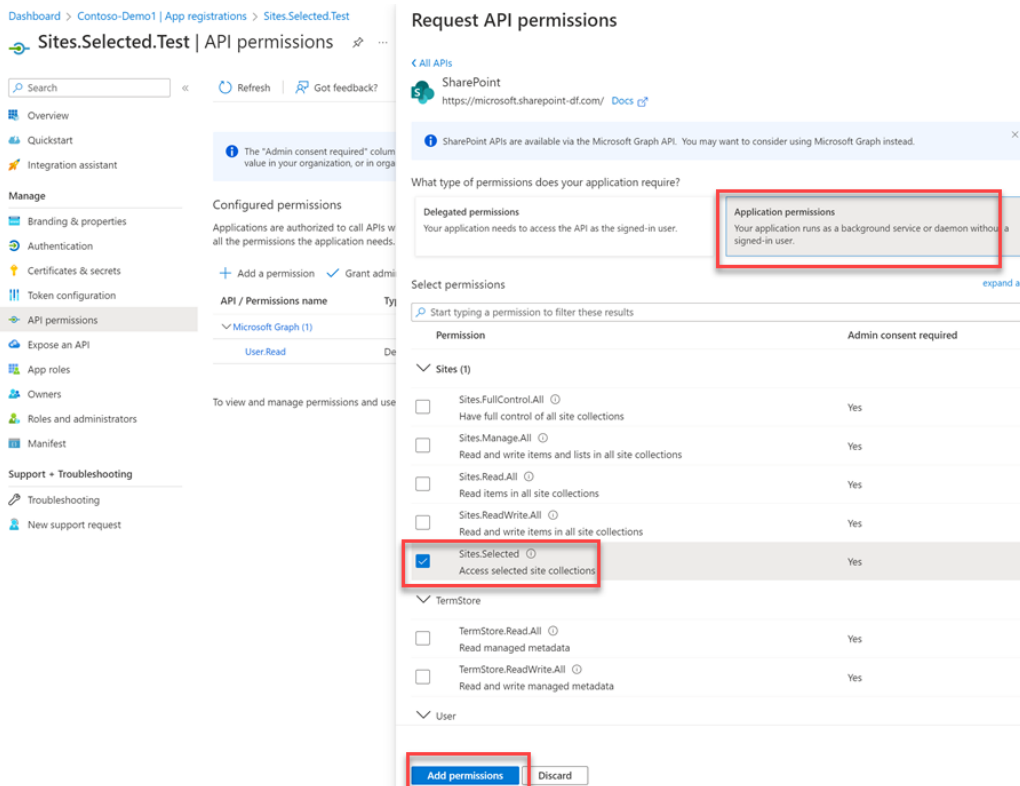
Upload certificate

Thumbprint	Description	Start date	Expires
CC9004B58960B74...	CN=SPOFullTrust	7/12/2020	7/12/2033

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"



- Select "Application permissions"
- Select "Sites.Selected" permission under "Site".
- Click "Add permission" button



Dashboard > Contoso-Demo1 | App registrations > Sites.Selected.Test

Sites.Selected.Test | API permissions

Search Refresh Got feedback?

You are editing permission(s) to your application, users will have to consent even if they've already done so previously.

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](#)

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 Contoso-Demo1

API / Permissions name	Type	Description	Admin consent req...	Status
Microsoft Graph (1)				
User.Read	Delegated	Sign in and read user profile	No	***
SharePoint (1)				
Sites.Selected	Application	Access selected site collections	Yes	⚠ Not granted for Contos... ***

To view and manage permissions and user consent, try [Enterprise applications](#).

- 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.

Dashboard > Contoso-Demo1 | App registrations > Sites.Selected.Test

Sites.Selected.Test | API permissions

Search Refresh Got feedback?

Grant admin consent confirmation.
Do you want to grant consent for the requested permissions for all accounts in Contoso-Demo1? This will update any existing admin consent records this application already has to match what is listed below.

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 Contoso-Demo1

API / Permissions name	Type	Description	Admin consent req...	Status
Microsoft Graph (1)				
User.Read	Delegated	Sign in and read user profile	No	***
SharePoint (1)				
Sites.Selected	Application	Access selected site collections	Yes	⚠ Not granted for Contos... ***

To view and manage permissions and user consent, try [Enterprise applications](#).

Dashboard > Contoso-Demo1 | App registrations > Sites.Selected.Test

Sites.Selected.Test | API permissions

Search Refresh Got feedback?

Overview
Quickstart
Integration assistant

Manage
Branding & properties
Authentication
Certificates & secrets
Token configuration
API permissions
Expose an API
App roles
Owners
Roles and administrators
Manifest

Support + Troubleshooting
Troubleshooting
New support request

Grant consent
Grant consent successful

Successfully granted admin consent for the requested permissions.

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](#)

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 Contoso-Demo1

API / Permissions name	Type	Description	Admin consent req...	Status
Microsoft Graph (1)				...
User.Read	Delegated	Sign in and read user profile	No	✓ Granted for Contoso-De...
SharePoint (1)				...
Sites.Selected	Application	Access selected site collections	Yes	✓ Granted for Contoso-De...

To view and manage permissions and user consent, try [Enterprise applications](#).

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

Register an application ...



* Name

The user-facing display name for this application (this can be changed later).

Sites.Selected.Operator



Supported account types

Who can use this application or access this API?

☒ Accounts in this organizational directory only (Contoso-Demo1 only - Single tenant)

☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant)

☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

☐ Personal Microsoft accounts only

[Help me choose...](#)

Redirect URI (optional)

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.

Select a platform



e.g. https://example.com/auth

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from [Enterprise applications](#).

By proceeding, you agree to the [Microsoft Platform Policies](#)

Register

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.

Dashboard > Contoso-Demo1 | App registrations > Sites.Selected.Operator

Sites.Selected.Operator | Certificates & secrets

Search Got feedback?

Overview
Quickstart
Integration assistant

Manage

- Branding & properties
- Authentication
- Certificates & secrets**
- Token configuration
- API permissions
- Expose an API
- App roles
- Owners
- Roles and administrators
- Manifest

Support + Troubleshooting

- Troubleshooting
- New support request

Update application credentials
Successfully updated application Sites.Selected.Operator credentials

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
default	3/25/2023	f1n8Q~WntYR4lo...	aad72217-4e7

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"

Dashboard > Contoso-Demo1 | App registrations > Sites.Selected.Operator

Sites.Selected.Operator | API permissions

Search Refresh Got feedback?

Overview
Quickstart
Integration assistant

Manage

- Branding & properties
- Authentication
- Certificates & secrets
- Token configuration
- API permissions**
- Expose an API
- App roles
- Owners
- Roles and administrators
- Manifest

Support + Troubleshooting

- Troubleshooting
- New support request

The "Admin consent required" checkbox reflects the value in your organization.

Configured permissions

Applications are authorized to call all the permissions the application has access to.

+ Add a permission

API / Permissions name

- Microsoft Graph (1)
- User.Read

To view and manage permissions

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 Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.

Azure Communication Services
Rich communication experiences with the same secure Cloud Managed Services platform used by Microsoft Teams

Azure DevOps
Integrate with Azure DevOps and Azure DevOps server

Azure Key Vault
Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults

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

Azure Storage
Secure, massively scalable object and data lake storage for unstructured and semi-structured data

Data Export Service for Microsoft Dynamics 365
Export data from Microsoft Dynamics CRM organization to an external destination

Dynamics 365 Business Central
Programmatic access to data and functionality in Dynamics 365 Business Central

Dynamics CRM
Access the capabilities of CRM business software and ERP systems

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

Dashboard > Contoso-Demo1 | App registrations > Sites.Selected.Operator

Sites.Selected.Operator | API permissions

Search Refresh Got feedback

Overview Quickstart Integration assistant

Manage

- Branding & properties
- Authentication
- Certificates & secrets
- Token configuration
- API permissions**
- Expose an API
- App roles
- Owners
- Roles and administrators
- Manifest

Support + Troubleshooting

- Troubleshooting
- New support request

Request API permissions

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

site

Permission Admin consent required

BrowserSiteLists

Sites (1)

Permission	Admin consent required
<input checked="" type="checkbox"/> Sites.FullControl.All Have full control of all site collections	Yes
<input type="checkbox"/> Sites.Manage.All Create, edit, and delete items and lists in all site collections	Yes
<input type="checkbox"/> Sites.Read.All Read items in all site collections	Yes
<input type="checkbox"/> Sites.ReadWrite.All Read and write items in all site collections	Yes

Add permissions Discard

Dashboard > Contoso-Demo1 | App registrations > Sites.Selected.Operator

Sites.Selected.Operator | API permissions

Search Refresh Got feedback

Overview Quickstart Integration assistant

Manage

- Branding & properties
- Authentication
- Certificates & secrets
- Token configuration
- API permissions**
- Expose an API
- App roles
- Owners
- Roles and administrators
- Manifest

Support + Troubleshooting

- Troubleshooting
- New support request

You are editing permission(s) to your application, users will have to consent even if they've already done so previously.

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](#)

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 Contoso-Demo1

API / Permissions name	Type	Description	Admin consent req...	Status
Microsoft Graph (2)				
Sites.FullControl.All	Application	Have full control of all site collections	Yes	Not granted for Contos...
User.Read	Delegated	Sign in and read user profile	No	

To view and manage permissions and user consent, try [Enterprise applications](#).

- 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.

Dashboard > Contoso-Demo1 | App registrations > Sites.Selected.Operator

Sites.Selected.Operator | API permissions

Search Refresh Got feedback?

Grant admin consent confirmation.
Do you want to grant consent for the requested permissions for all accounts in Contoso-Demo1? This will update any existing admin consent records this application already has to match what is listed below.

Yes No

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 Contoso-Demo1

API / Permissions name	Type	Description	Admin consent req...	Status
Microsoft Graph (2)				...
Sites.FullControl.All	Application	Have full control of all site collections	Yes	⚠ Not granted for Contos_...
User.Read	Delegated	Sign in and read user profile	No	...

To view and manage permissions and user consent, try [Enterprise applications](#).

Support + Troubleshooting
Troubleshooting
New support request

Dashboard > Contoso-Demo1 | App registrations > Sites.Selected.Operator

Sites.Selected.Operator | API permissions

Search Refresh Got feedback?

Successfully granted admin consent for the requested permissions.

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](#)

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 Contoso-Demo1

API / Permissions name	Type	Description	Admin consent req...	Status
Microsoft Graph (2)				...
Sites.FullControl.All	Application	Have full control of all site collections	Yes	✓ Granted for Contoso-De_...
User.Read	Delegated	Sign in and read user profile	No	✓ Granted for Contoso-De_...

To view and manage permissions and user consent, try [Enterprise applications](#).

Support + Troubleshooting
Troubleshooting
New support request

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.
```

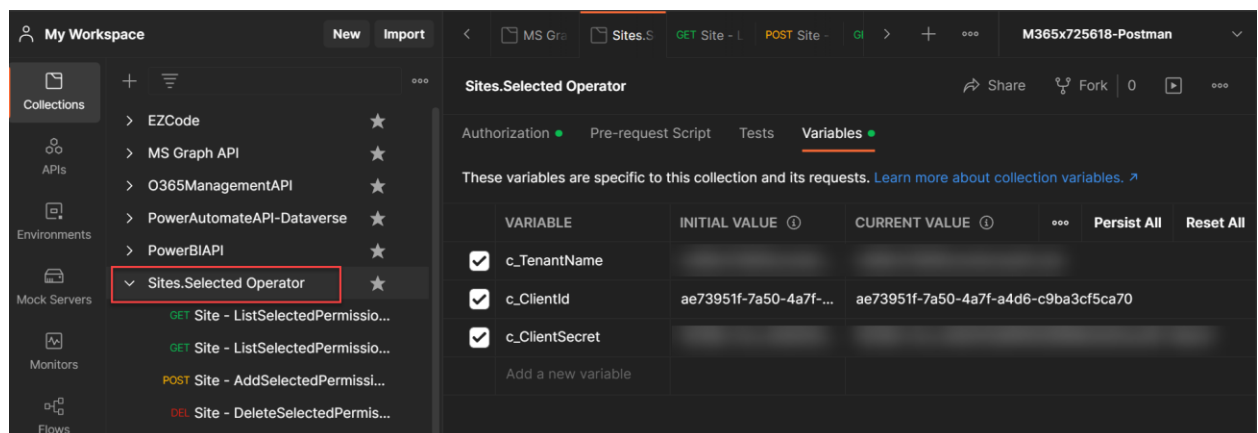
```
# permissions: it can be read or write
```

```
Grant-PnPAzureADAppSitePermission -AppId "aa37b89e-75a7-47e3-bdb6-b763851c61b6" -DisplayName
"Site.Selected.Test" -Permissions Read
```

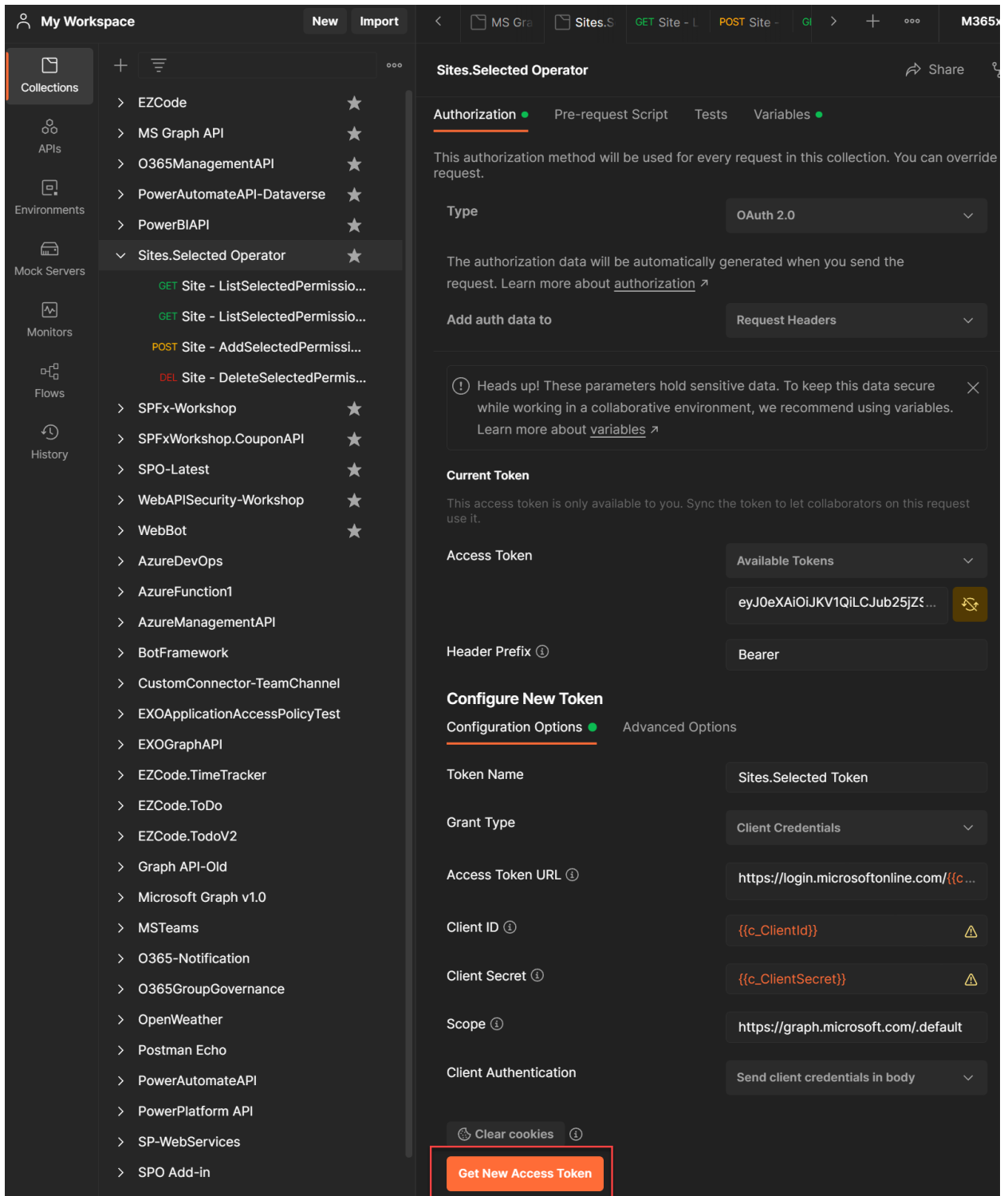
Grant Azure AD application to site collection via MS Graph API

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:

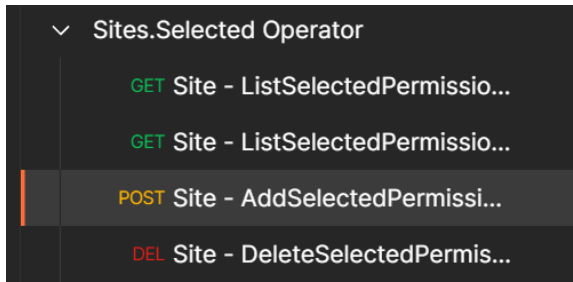
1. Download Postman collection json from [SPOSitesSelected](#)
2. Click "File" -> "Import" menu to import json file which you download from above step.
3. Click "..." right beside the collection name and click "Edit" context menu to bring up the collection property window. Select "Variables" tab and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



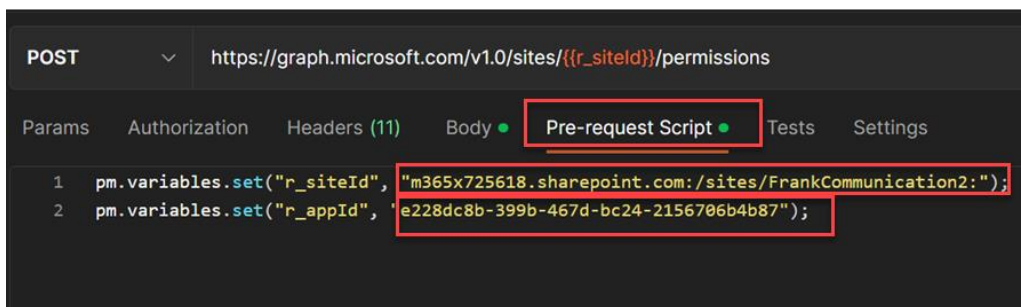
4. Select "Authorization" tab, then click "Get New Access Token" to generate the access token



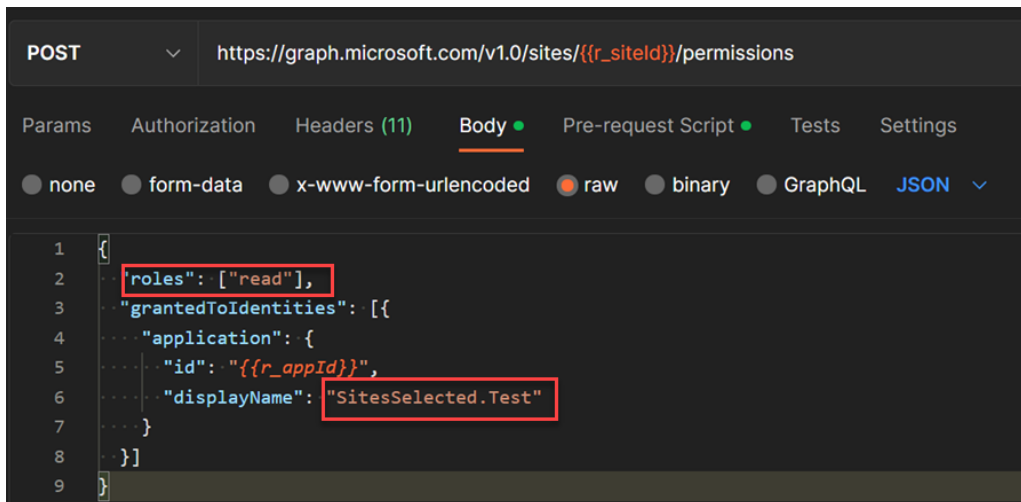
5. Select “Site - AddSelectedPermissions” request. The request detail information is shown up.



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.

POST

https://graph.microsoft.com/v1.0/sites/{{r_siteId}}/permissions

Send

Params

Auth

Headers (11)

Body

Pre-req.

Tests

Settings

Cookies

raw

JSON

Beautify

```
1 {
2   "roles": ["read"],
3   "grantedToIdentities": [{
4     "application": {
5       "id": "{{r_appId}}",
6       "displayName": "SitesSelected.Test"
7     }
8   }]
9 }
```

Body

201 Created 1165 ms 1.67 KB

Save Response

Pretty

Raw

Preview

Visualize

JSON

```
1 {
2   "@odata.context": "https://graph.microsoft.com/v1.0/$metadata#Collection(microsoft.graph.permission)/$entity",
3   "id": "aTowaS50fG1zLnNwLmV4dHx1MjI4ZGM4Yi0zOTliLTQ2N2QtYmMyNC0yMTU2NzA2YjRiODdAOGE1ZWUzNTctN2RlMC00ODM2LWFiMjAtOTE3M2IxMmNkY2U5",
4   "roles": [
5     "read"
6   ],
7   "grantedToIdentitiesV2": [
8     {
9       "application": {
10        "displayName": "SitesSelected.Test",
11        "id": "e228dc8b-399b-467d-bc24-2156706b4b87"
12      }
13    }
14  ],
15  "grantedToIdentities": [
16    {
17      "application": {
18        "displayName": "SitesSelected.Test",
19        "id": "e228dc8b-399b-467d-bc24-2156706b4b87"
20      }
21    }
22  ]
23 }
```

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
```

```
PS C:\AzureDevOps\PFEPProjects-Private\PS-Samples> $siteUrl = "https://[redacted].sharepoint.com/sites/FrankCommunication2"
Connect-PnPOnline -Url $siteUrl `
  -ClientId [redacted] 4b87 `
  -Tenant [redacted].onmicrosoft.com `
  -Thumbprint [redacted] 397e

PS C:\AzureDevOps\PFEPProjects-Private\PS-Samples>
PS C:\AzureDevOps\PFEPProjects-Private\PS-Samples> Get-PnPWeb

Title                ServerRelativeUrl      Id
-----                -
FrankCommunication2  /sites/FrankCommunication2  d90eb8ac-7603-4edf-be40-45c6bdf947cd
```