

1. **Create** and Register a new single tenant App Registration in Entra ID.

[Home](#) > [Contoso](#) | [App registrations](#) >

Register an application

* Name

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

Muhimbi SPFx App Registration ✓

Supported account types

Who can use this application or access this API?

- ☒ Accounts in this organizational directory only (Contoso only - Single tenant)
- ☐ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)
- ☐ Accounts in any organizational directory (Any Microsoft Entra ID tenant - 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

2. **Create** a self signed certificate on your local machine using the powershell script found [here](#).

Copy the script linked above,

Paste into a text editor (e.g NotePad).

Save as a .ps1 file e.g Create-SelfSignedCertificate.ps1

Start Windows PowerShell as Administrator and navigate to the script location

Execute the command

```
.\Create-SelfSignedCertificate.ps1 -CommonName "MyCompanyName" -StartDate 2024-09-19  
-EndDate 2025-09-18
```

You will be asked to give a password to encrypt your private key, then both the .PFX file and .CER file will be generated and exported to the current folder.

It is not advisable to use special characters in the encryption password.

Please provide your company name or domain in -CommonName

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\WINDOWS\system32> cd \
PS C:\> cd .\Certificate\
PS C:\Certificate> .\Create-SelfSignedCertificate.ps1 -CommonName "MuhimbiAppRegCert1" -StartDate 2024-09-19 -EndDate 2025-09-18
Enter Password to protect private key: *****

Directory: C:\Certificate

Mode                LastWriteTime         Length Name
----                -
-a----          9/19/2024   3:41 AM           2633 MuhimbiAppRegCert1.pfx
-a----          9/19/2024   3:41 AM           782  MuhimbiAppRegCert1.cer

PS C:\Certificate>
```

For more information on creating Self signed certificates, see [this Microsoft article](#).


3. Associate the self signed certificate (.cer) with the app registration created in STEP 1 above.
 - In Entra ID, go to App Registrations. (If you do not see it in your Owned Applications, go to All Applications.)
 - Open the App registration you created and click on Add a Certificate or Secret.



- Click on Certificates -> Upload certificate
Use the folder button in front of the Upload field to bring up the Open dialog box, navigate to where your .cer file is located and click Open.

Upload certificate

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



Description

Muhimbi App Certificate

After selecting your certificate and entering a description(Optional), click Add.

4. Add the permissions for the app

After adding the certificate, on the left hand side menu, Select API Permissions to grant the required permissions for the app.

i) Add a Permission -> Microsoft Graph -> Application Permissions

- Sites.FullControl.All

- User.Read.All

Click Add/Update Permissions

ii) Add a Permission -> SharePoint -> Application Permissions

- AllSites.FullControl

- User.Read.All

Click Add/Update Permissions

Home > Contoso | App registrations > Muhimbi SPFx App Registration

Muhimbi SPFx App Registration | API permissions

Search Refresh Got feedback?

- 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

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](#)

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (3)				
Sites.FullControl.All	Application	Have full control of all site collections	Yes	⚠ Not granted for Contoso
User.Read	Delegated	Sign in and read user profile	No	...
User.Read.All	Application	Read all users' full profiles	Yes	⚠ Not granted for Contoso
SharePoint (2)				
Sites.FullControl.All	Application	Have full control of all site collections	Yes	⚠ Not granted for Contoso
User.Read.All	Application	Read user profiles	Yes	⚠ Not granted for Contoso

As you can see the status of all Permissions show a warning that it needs Admin Consent.

Click on the Grant Admin Consent and the Status should all show green checkmarks.

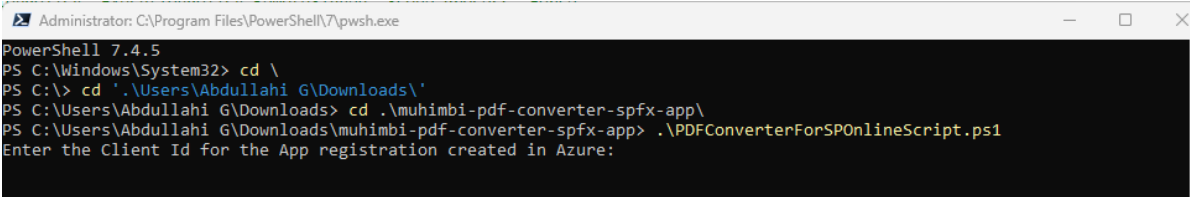
Configured permissions

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](#) ←

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (3)				
Sites.FullControl.All	Application	Have full control of all site collections	Yes	✓ Granted for Contoso
User.Read	Delegated	Sign in and read user profile	No	✓ Granted for Contoso
User.Read.All	Application	Read all users' full profiles	Yes	✓ Granted for Contoso
SharePoint (2)				
Sites.FullControl.All	Application	Have full control of all site collections	Yes	✓ Granted for Contoso
User.Read.All	Application	Read user profiles	Yes	✓ Granted for Contoso

5. Ensure you have the latest version of PowerShell installed before running the script. To install the latest version of Powershell, please visit <https://learn.microsoft.com/en-us/powershell/scripting/install/installing-powershell-on-windows?view=powershell-7.4>
6. Open Powershell 7 as Admin (goto Start menu and type pwsh. You will see PowerShell 7.x.x)
 - If you do not have it imported already, import PnP.PowerShell module using the command *Import-Module PnP.PowerShell*.
PS: If you just installed Powershell 7, please run this command to import the latest version of PowerShell.
Windows Powershell less than version 7 does not support the latest PnP.PowerShell module, so PowerShell 7 is required.
7. Run the Script provided to install the SPFx App in your tenant.
 - The script requires the ClientID of the App registration created in STEP 1.
 - The full path to the .pfx self signed certificate e.g
C:\folderName\certificateName.pfx
 - The Password used to create the certificate
 - Your tenant URL. To confirm, click on the gear icon in portal.azure.com and check the Domain field.
 - Navigate to where the script is located and execute the script with the command
.\PDFConverterForSPOnlineScript.ps1



```
Administrator: C:\Program Files\PowerShell\7\pwsh.exe
PowerShell 7.4.5
PS C:\Windows\System32> cd \
PS C:\> cd '.\Users\Abdullahi G\Downloads\'
PS C:\Users\Abdullahi G\Downloads> cd .\muhimbi-pdf-converter-spfx-app\
PS C:\Users\Abdullahi G\Downloads\muhimbi-pdf-converter-spfx-app> .\PDFConverterForSPOnlineScript.ps1
Enter the Client Id for the App registration created in Azure:
```

8. While running the script if you encounter below error
FilePath\PDFConverterForSPOnlineScript.ps1 cannot be loaded. The file
FilePath\PDFConverterForSPOnlineScript.ps1 is not digitally signed. You cannot
run this script on the current system.

Please make sure you have set the execution policy

```
Set-ExecutionPolicy -ExecutionPolicy RemoteSigned -Scope Process -Force
```

If you still encounter the same error please execute below command

```
Unblock-File -Path FilePath\PDFConverterForSPOnlineScript.ps1
```

