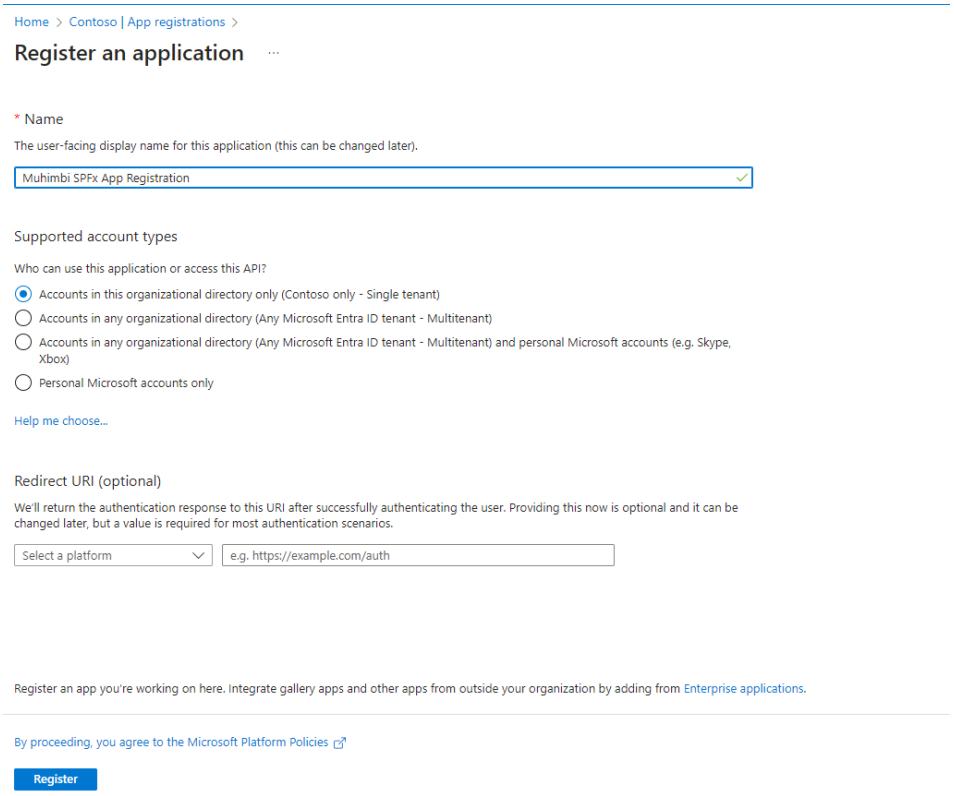
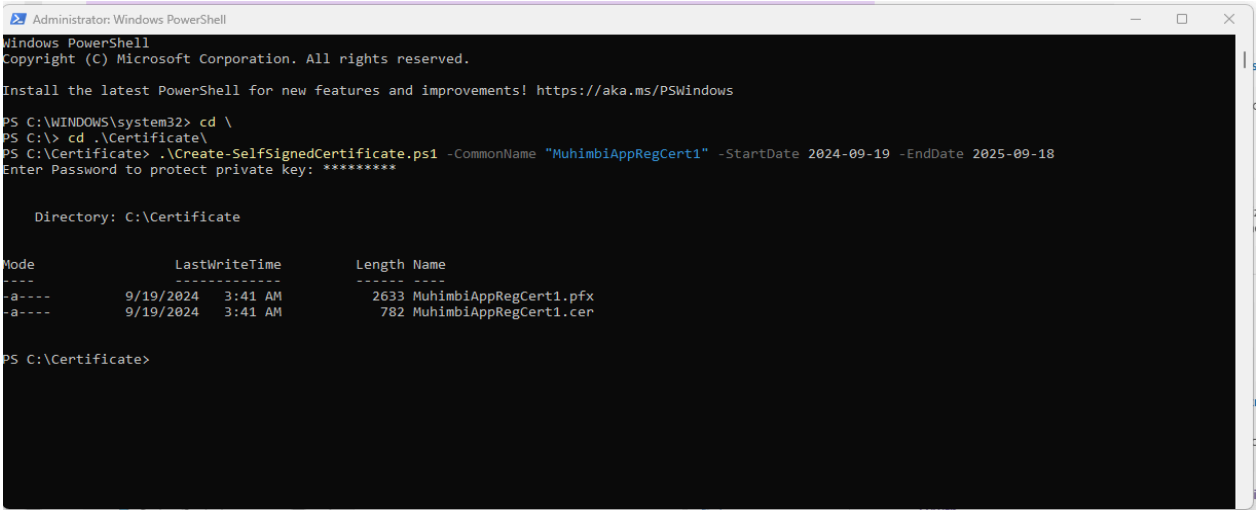
1. **Create** and Register a new single tenant App Registration in Entra ID.



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

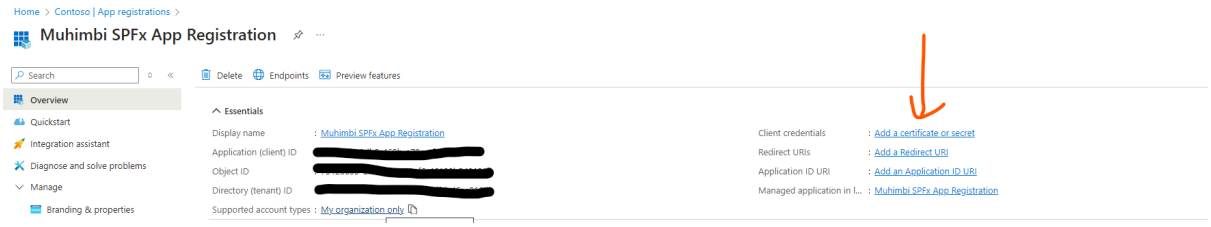
   You will be asked to give a password to encrypt your private key, then both the .PFX file and .CER file will be generated and exported to the current folder.
   It is not advisable to use special characters in the encryption password.
   Please provide your company name or domain in -CommonName



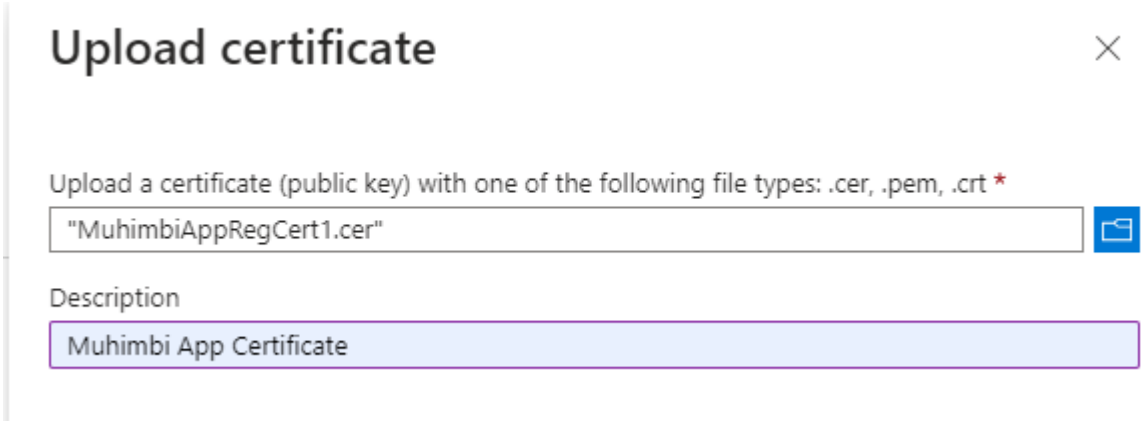
For more information on creating Self signed certificates, see this Microsoft article.

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 fron of the Upload field to bring up the Open dialog box, navigate to where your .cer file is located and click Open.



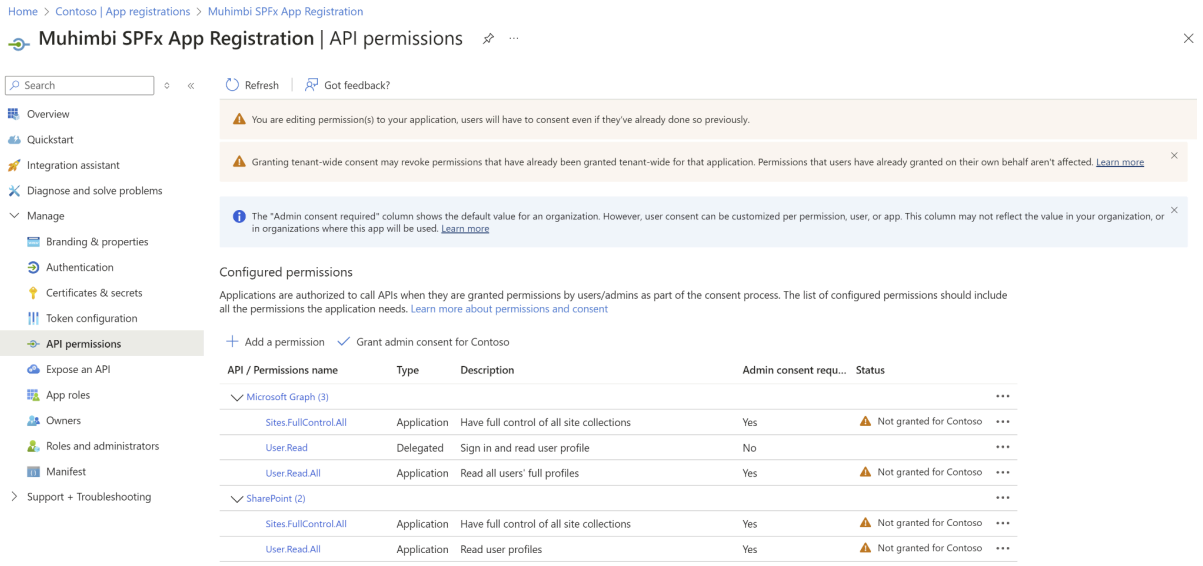
After selecting your certificate and entering a desciption(Optional), click Add.

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

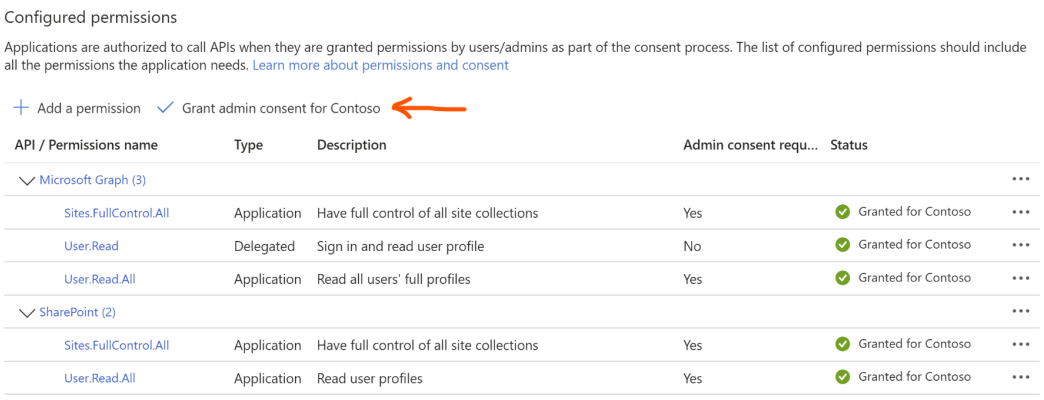
   Click Add/Update Permissions

   ii) Add a Permission -> SharePoint -> Application Permissions
   - AllSites.FullControl
   - User.Read.All

   Click Add/Update Permissions



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.

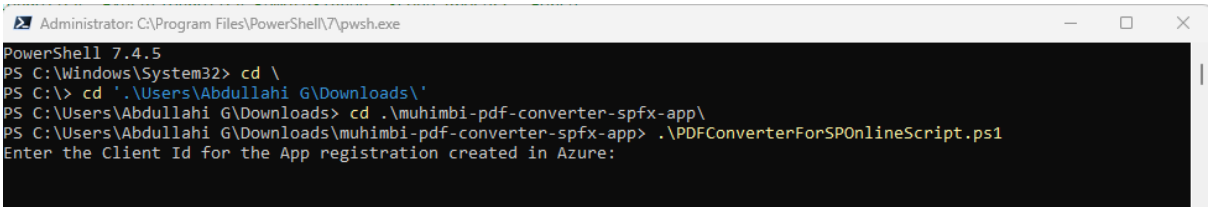


5. Ensure you have the latest version of PowerShell installed before running the script. To install the latest version of Powershell, please visit https://learn.microsoft.com/en-us/powershell/scripting/install/installing-powershell-on-windows?view=powershell-7.4

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



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
   ```