

Azure App Registration Step by Step

Step 1

Creating an Azure App Registration involves a few steps.

1. Sign in to the Azure portal using an account with administrator permissions.
2. In the left navigation pane, select App registrations.
3. Click on + New registration to create a new app registration.
4. Provide the following information:
 - Name: Enter a display name for your application.
 - Supported account types: Specify who can use the application (e.g., accounts in this organizational directory only, or any account).
 - Redirect URI (optional): Although optional, it's necessary for most scenarios.
5. Click Register to create the application registration.
6. Note down the Application (client) ID and Directory (tenant) ID. You'll need these for authentication.

Step : 2

To create a client ID and client secret for an Azure App Registration, follow these steps:

1. Sign in to the Azure portal using an account with administrator permissions.
2. In the left navigation pane, select Azure Active Directory.
3. Click on App registrations.
4. Choose the application for which you want to create the client secret.
5. Navigate to Certificates & secrets from the left navigation.
6. Select the Client secrets tab.
7. Click New client secret, provide a description, and set an expiration duration.
8. Click Add to create the client secret.

Step: 3

To add API permissions to an Azure App Registration, follow these steps:

1. Go to App Registration: Open the app registration you have created.
2. Navigate to API Permissions: On the left-hand side, click on "API permissions".
3. Add a Permission: Click on "Add a permission".
4. Configure Access : Provide the access as per the required settings.
5. Add API Permissions: As per given below screenshot

Home > App registrations > SP2AzureBlob

SP2AzureBlob | 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

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 katproe5

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (8)				
Files.ReadWrite.All	Delegated	Have full access to all files user can access	No	Granted for katproe5
Sites.FullControl.All	Delegated	Have full control of all site collections	Yes	Granted for katproe5
Sites.FullControl.All	Application	Have full control of all site collections	Yes	Granted for katproe5
Sites.Manage.All	Application	Create, edit, and delete items and lists in all site collections	Yes	Granted for katproe5
Sites.Read.All	Application	Read items in all site collections	Yes	Granted for katproe5
Sites.ReadWrite.All	Application	Read and write items in all site collections	Yes	Granted for katproe5
Sites.Selected	Application	Access selected site collections	Yes	Granted for katproe5
User.Read	Delegated	Sign in and read user profile	No	Granted for katproe5
SharePoint (4)				
AllSites.FullControl	Delegated	Have full control of all site collections	Yes	Granted for katproe5
MyFiles.Read	Delegated	Read user files	No	Granted for katproe5
MyFiles.Write	Delegated	Read and write user files	No	Granted for katproe5
Sites.FullControl.All	Application	Have full control of all site collections	Yes	Granted for katproe5

To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try [Enterprise applications](#).

6. One you have added the API Permissions Click on Grant Admin Consent

SP2AzureBlob | 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

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 katproe5

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (8)				
Files.ReadWrite.All	Delegated	Have full access to all files user can access	No	✓ Granted for katproe5
Sites.FullControl.All	Delegated	Have full control of all site collections	Yes	✓ Granted for katproe5
Sites.FullControl.All	Application	Have full control of all site collections	Yes	✓ Granted for katproe5
Sites.Manage.All	Application	Create, edit, and delete items and lists in all site collections	Yes	✓ Granted for katproe5
Sites.Read.All	Application	Read items in all site collections	Yes	✓ Granted for katproe5
Sites.ReadWrite.All	Application	Read and write items in all site collections	Yes	✓ Granted for katproe5