# Using Graph APIs and Azure Applications in SharePoint Framework Solutions

* Client-side applications that are incapable of storing a secret, such as SharePoint Framework solutions, use a specific type of OAuth flow named [OAuth implicit flow](https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-dev-understanding-oauth2-implicit-grant).

## Connect to MS Graph

* Microsoft confirmed that the permissions granted in this scenario are **Delegated.** Users can only perform actions on M365 resources they already have access to do so.
* The permissions must be requested through SPFx solution and need to be granted through **SharePoint Admin Center**. Once permissions are granted, they are available across the tenant and not specific to requesting solution. Those permissions will be available for other solutions as well. Removing solution will not revoke permissions.
* Permission request doesn't affect solution deployment. Solution deployment will work but graph API functions will not work.
* Revoking previously granted permissions doesn't invalidate issued access tokens. Access tokens will need to be expired.
* Internally SharePoint Online is using out of the box Azure App called **SharePoint Online Client Extensibility** to set the permissions.
* It is possible to enable/disable API usage for SPFx solutions in the tenant using **Disable-SPOTenantServicePrincipal**
* References
  + <https://docs.microsoft.com/en-us/sharepoint/dev/spfx/use-msgraph>
  + [Consume MS Graph - Tutorial](https://docs.microsoft.com/en-us/sharepoint/dev/spfx/use-aad-tutorial)

## Connect to Azure API

* It is possible to use Azure APIs in SPFx solution through App registrations.
* Permissions will be granted to Azure AD Application registration which will access Azure API through SPFx.
* References
  + <https://docs.microsoft.com/en-us/sharepoint/dev/spfx/use-aadhttpclient>