Microsoft Graph:

Following the document.

https://developer.microsoft.com/en-us/graph/docs/concepts/auth\_v2\_user

The basic steps required are:

1. Register your app with Azure AD.

Register your app at **Azure App registrations** settings in the **Azure Portal**.  
You can use either a Microsoft account or a work or school account to register your app.

* Click on the **+ New registration** button to create a new app
* Select a name for the app and the account types who should be accessible to this API
* Set <http://localhost> as the Redirect URI
* Click on **Register** button
* On the main app page, copy the **Application (client) ID** and the **Directory (tenant) ID**
* Go to the API permissions settings and click on **+ Add a permission** button
* Add the following permissions:
  + Microsoft Graph -> Application permissions -> User.ReadWrite.All
  + Microsoft Graph -> Application permissions -> Mail.Read
  + Microsoft Graph -> Application permissions -> Directory.ReadWrite.All
  + Microsoft Graph -> Delegated permissions -> Directory.AccessAsUser.All
  + Microsoft Graph -> Application permissions -> SecurityEvents.ReadWrite.All
  + Microsoft Graph -> Application permissions -> SecurityEvents.Read.All
* Click on **Grant admin consent** to grant access for Siemplify to the API.
* Go to **Certificates & secrets** and create a new Client Secret for Siemplify to use. Set it to never expire. Copy the generated Client Secret value.

1. Configure **Microsoft Graph** Integration with the following values from the previous step:

* Client ID = Application (client) ID
* Tenant: Directory (tenant) ID
* Secret ID: Client Secret