**Azure Configuration**

1)     Go to aad.portal.azure.com

2)     Click on Azure Active Directory

3)     Click on App Registrations

Graphical user interface, application, Teams

Description automatically generated

4)     Click ‘New Registration’

5)     Provide a name for your app

6)     Specify supported account types (default will function in most scenarios)

7)     Specify <https://us.nintex.io/connection/api/Token> as the Redirect URI for the app (this will be used for authentication)

8)     Click ‘Register’

9)     Click on API Permissions

10)  Click Add a permission

11)  Click on Azure Active Directory Graph

12)  Click on Delegated Permissions

13)  Check the boxes for the Scopes below. Scopes will be found under their specific name groups eg User.ReadBasic.All will be under the user option

* "User.ReadBasic.All"
* "User.Read.All”
* "User.Read"
* "Files.Read"
* "Files.Read.All"

14)  Click ‘Add Permissions’ once all scopes have been added.

15)  Click ‘Grant admin consent’ button

16)  Click on Certificates and Secrets

17)  Click ‘New Client Secret

18)  Copy the secret. This will be used in configuring the Xtension in Nintex Workflow Cloud. KEEP THIS WINDOW OPEN

19)  Upload the Xtension to Nintex Workflow Cloud (login and click ‘Xtensions’)

20)  Specify ‘Microsoft Graph’ for the Security drop down

21)  Paste the Client Secret from step 18

22)  Go Back to your window with your app in Azure AD portal and click Overview

23)  Click on the copy button next to the Application ID

24)  Go back to your Xtension configuration

25)  Paste the client ID you just copied in to the ‘Client ID’ field

26)  Hit the ‘Next’ button’

27)  Specify a name (if different) for the group of Azure AD actions and upload an image for the connector.

28)  Click publish.

29)  The Get Excel Workbook ID will now be available in your NWC tenant! For configuration you will drag and drop your new Azure AD actions in to the workflow canvas and Configure a connection. This will use the permissions granted in the previous steps via a delegated authentication auth flow.