# 1 Add new Client

Login to Azure Active Directory. In the left menu, click App registrations.

Click “New registration”. Set the following

Name: NGOBIA IDP TRN

On Redirect URI, select Web and set value to: **https://dpwh-ngobia-idp-trn.movementsoft.com/signin-aad/**

Once created, set the Front-channel logout URL value to:

**https://dpwh-ngobia-idp-trn.movementsoft.com/signout-aad/**

You need to change it as needed.

# 2 Create Client Secret (NGOBIA IDP TRN)

Under Certificates & secrets, click “New client secret”.

A screenshot of a computer screen

Description automatically generated

Description: NGOBIA secret

Expires: 24 months

Create the secret, then once created take note of the Value. We will need this soon.

# 3 Configure API permissions

Click API permissions in the blade menu.

1. Click Add permission.
2. Click Microsoft Graph
3. Select Delegated permissions
4. Select OpenId permissions as shown below:

A screenshot of a computer

Description automatically generated

# 4 In the end we need the following details:

* Client ID
* Tenant ID
* Redirect URIs
* Logout URIs
* Client Secrets

**Sample:**

Client ID: b3cc335e-680b-47be-a61a-c490250fbc2b

Tenant ID: 37feda23-8c9a-4f00-9597-74e5b0abeb3a

Redirect URIs: https://dpwh-ngobia-idp-trn.movementsoft.com/signin-aad/

Logout URIs: https://dpwh-ngobia-idp-trn.movementsoft.com/signout-aad/

Client Secret: WHF8Q~Q~PjbPMTjK-SapCqhlewG1P9W6rDNvPc\_~