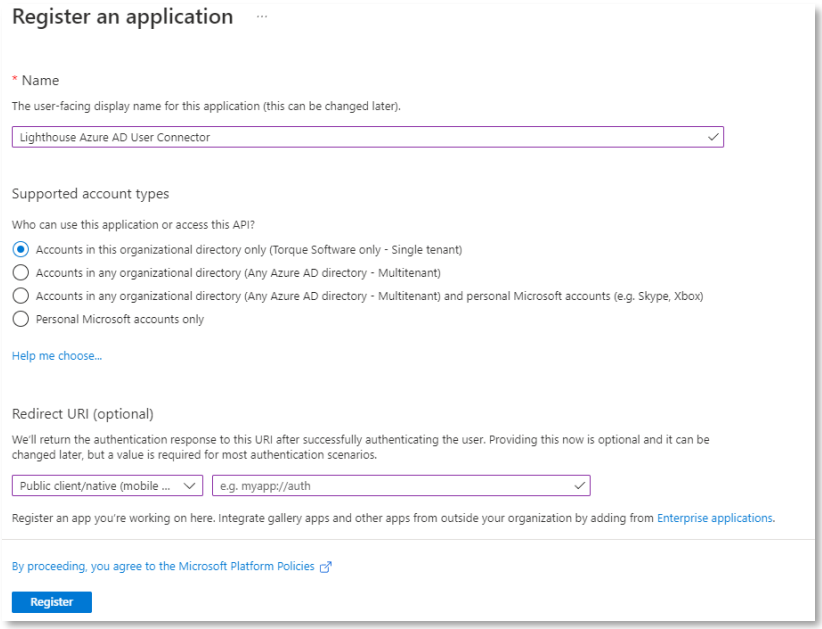
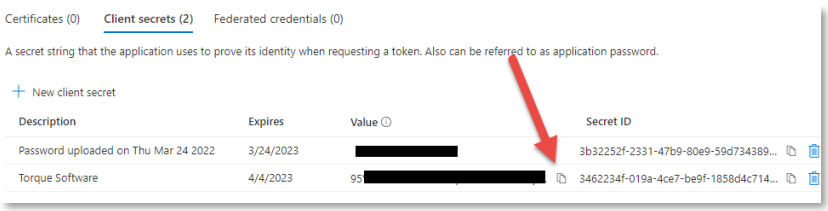
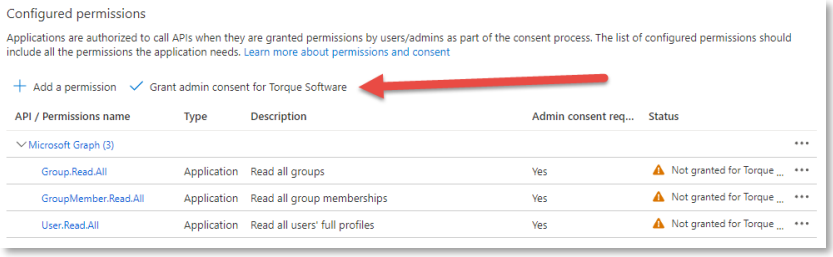
Register Lighthouse in Azure Active Directory

1. Open your Azure Portal and select '**Azure Active Directory'**
2. On the left, select '**App registrations'**
3. Click **'New registration'**
    a. Enter the name - "Lighthouse Azure AD User Connector"
    b. Select '**Accounts in this organizational directory only'**
    c. You can leave the Redirect URI blank
    d. Click '**Register'.**
4. Once created, click on '**Certificates & secrets'** in the left-hand menu
    a. Click '**New client secret'**
    b. Provide a name, e.g. *"Torque Lighthouse"*
    c. Set the '**Expires'** value to the lesser of your Torque Software contract duration or your cybersecurity policy for secret key issuance
    d. Select '**Add'**
    e. When created, click the copy icon and save this value securely somewhere (note: it will not be accessible after you leave this step).
5. Select '**API permissions'** from the left-hand menu
    a. Click '**+ Add a permission'**
    b. Select '**Microsoft Graph'**
    c. Select '**Application permissions'**
    d. Search for and '**add'** the following permissions:
        i. Group.Read.All
        ii. GroupMember.Read.All
        iii. User.Read.All
    e. When back on the Configured permissions view, click '**Grant admin consent for Torque Software'**
    f. Select '**Yes'** to the confirmation pop up to grant admin consent.







Azure AD is now successfully configured for your Lighthouse instance. If you would like to limit the users in your Azure AD tenancy to those in a specific group, follow the steps below.

Restrict Lighthouse Users to a Specific Group (optional)

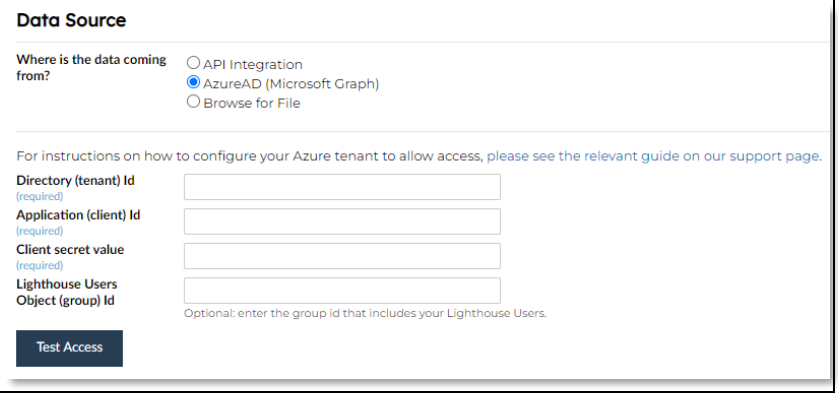
1. Select '**Home**' in the top left
2. Select '**Azure Active Directory**'
3. Select '**Groups**' from the left-hand menu
4. Select '**New group**'
    a. Leave '**Group type**' as '**Security**'
    b. Enter *"Lighthouse Users"* as the '**Group name**'
    c. Enter a meaningful description for your administrative purposes
    d. Click on '**No members selected**' and add all the relevant users
    e. Click '**Create**'.

Configure Lighthouse to Integrate with Azure AD

Once you have carried out the steps above, you will have everything you need to integrate Lighthouse with Azure AD.

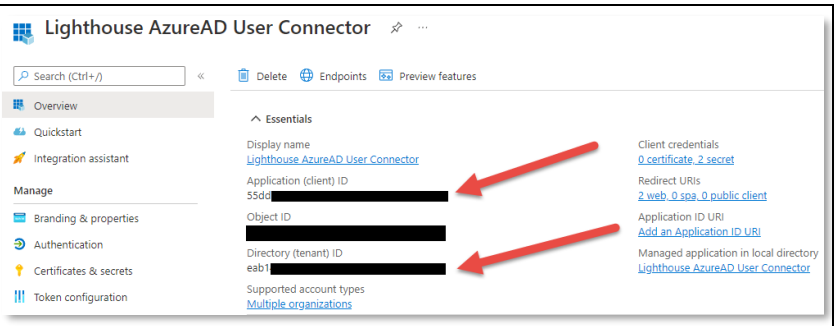
Note: you must be in the '**Data connection administrators**' and '**User and Organisation unit management team**' groups (found under **System Settings**, on the **Permissions/Workflow** tab).

1. Select the Settings cog icon
2. Select '**Administration**'
3. Select '**Import/Export User and Organisational Structure**'
4. Click '**Add Data Source**'
5. Select '**Azure AD (Microsoft Graph)**'



6. From the “Lighthouse Azure AD User Connector" app registration overview page in Azure AD (created in the first section of this document), copy and paste the relevant values into the fields in Lighthouse:
    a. Copy and paste the ‘**Directory (tenant) ID’**
    b. Copy and paste the ‘**Application (client) ID’**
    c. Paste the ‘**Secret value’** created in step 2 of this document into the ‘**Client secret value’** field
    d. If you configured a group to limit your users in the second section of this document, copy and paste the ‘**Object Id’** from the group overview page into the ‘**Lighthouse Users Object (group) Id’** field
    e. Click ‘**Test Access’.**

If there is a problem, testing access it should let you know what it is, and give you ideas on how to remedy it. If the test succeeds, please continue configuring your import as per the user guide.



TORQUE
SOFTWARE