

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.

Register an application

* Name
The user-facing display name for this application (this can be changed later).
Lighthouse Azure AD User Connector

Supported account types
Who can use this application or access this API?
 Accounts in this organizational directory only (Torque Software only - Single tenant)
 Accounts in any organizational directory (Any Azure AD directory - Multitenant)
 Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
 Personal Microsoft accounts only
[Help me choose...](#)

Redirect URI (optional)
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.
Public client/native (mobile ... | e.g. myapp://auth

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from [Enterprise applications](#).

By proceeding, you agree to the [Microsoft Platform Policies](#)

Register

Certificates (0) **Client secrets (2)** Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description	Expires	Value	Secret ID
Password uploaded on Thu Mar 24 2022	3/24/2023	[REDACTED]	3b32252f-2331-47b9-80e9-59d734389...
Torque Software	4/4/2023	95 [REDACTED]	3462234f-019e-4ce7-be9f-1858d4c714...

Configured permissions
Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission Grant admin consent for Torque Software

API / Permissions name	Type	Description	Admin consent req...	Status
Microsoft Graph (3)				
Group.Read.All	Application	Read all groups	Yes	⚠ Not granted for Torque ...
GroupMember.Read.All	Application	Read all group memberships	Yes	⚠ Not granted for Torque ...
User.Read.All	Application	Read all users' full profiles	Yes	⚠ Not granted for Torque ...



<p>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.</p>	
<p>Restrict Lighthouse Users to a Specific Group (optional)</p> <ol style="list-style-type: none"> 1. Select 'Home' in the top left 2. Select 'Azure Active Directory' 3. Select 'Groups' from the left-hand menu 4. Select 'New group' <ol style="list-style-type: none"> a. Leave 'Group type' as 'Security' b. Enter <i>"Lighthouse Users"</i> 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'. 	
<p>Configure Lighthouse to Integrate with Azure AD</p> <p>Once you have carried out the steps above, you will have everything you need to integrate Lighthouse with Azure AD.</p> <p>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).</p> <ol style="list-style-type: none"> 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)' 	<div data-bbox="699 1592 1516 1948"> <p>Data Source</p> <p>Where is the data coming from? <input type="radio"/> API Integration <input checked="" type="radio"/> AzureAD (Microsoft Graph) <input type="radio"/> Browse for File</p> <p>For instructions on how to configure your Azure tenant to allow access, please see the relevant guide on our support page.</p> <p>Directory (tenant) Id (required) <input type="text"/></p> <p>Application (client) Id (required) <input type="text"/></p> <p>Client secret value (required) <input type="text"/></p> <p>Lighthouse Users Object (group) Id <input type="text"/></p> <p>Optional: enter the group id that includes your Lighthouse Users.</p> <p>Test Access</p> </div>



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.

The screenshot displays the 'Lighthouse AzureAD User Connector' app registration overview page. The 'Essentials' section is visible, showing the following fields and values:

- Display name: [Lighthouse AzureAD User Connector](#)
- Application (client) ID: 55dc[redacted]
- Object ID: [redacted]
- Directory (tenant) ID: eab1[redacted]
- Supported account types: [Multiple organizations](#)

On the right side, there are links for 'Client credentials', 'Redirect URIs', and 'Application ID URI'. Two red arrows point to the 'Application (client) ID' and 'Directory (tenant) ID' fields.

TORQUE
SOFTWARE

