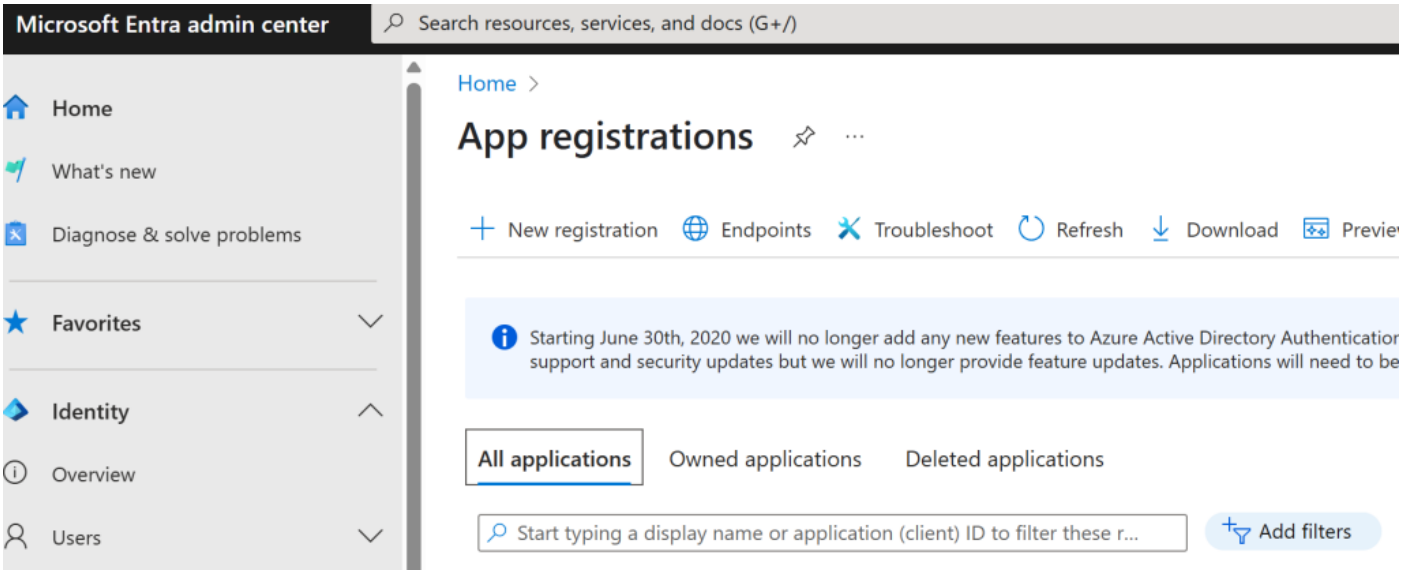
# Connect to O365 Sharepoint

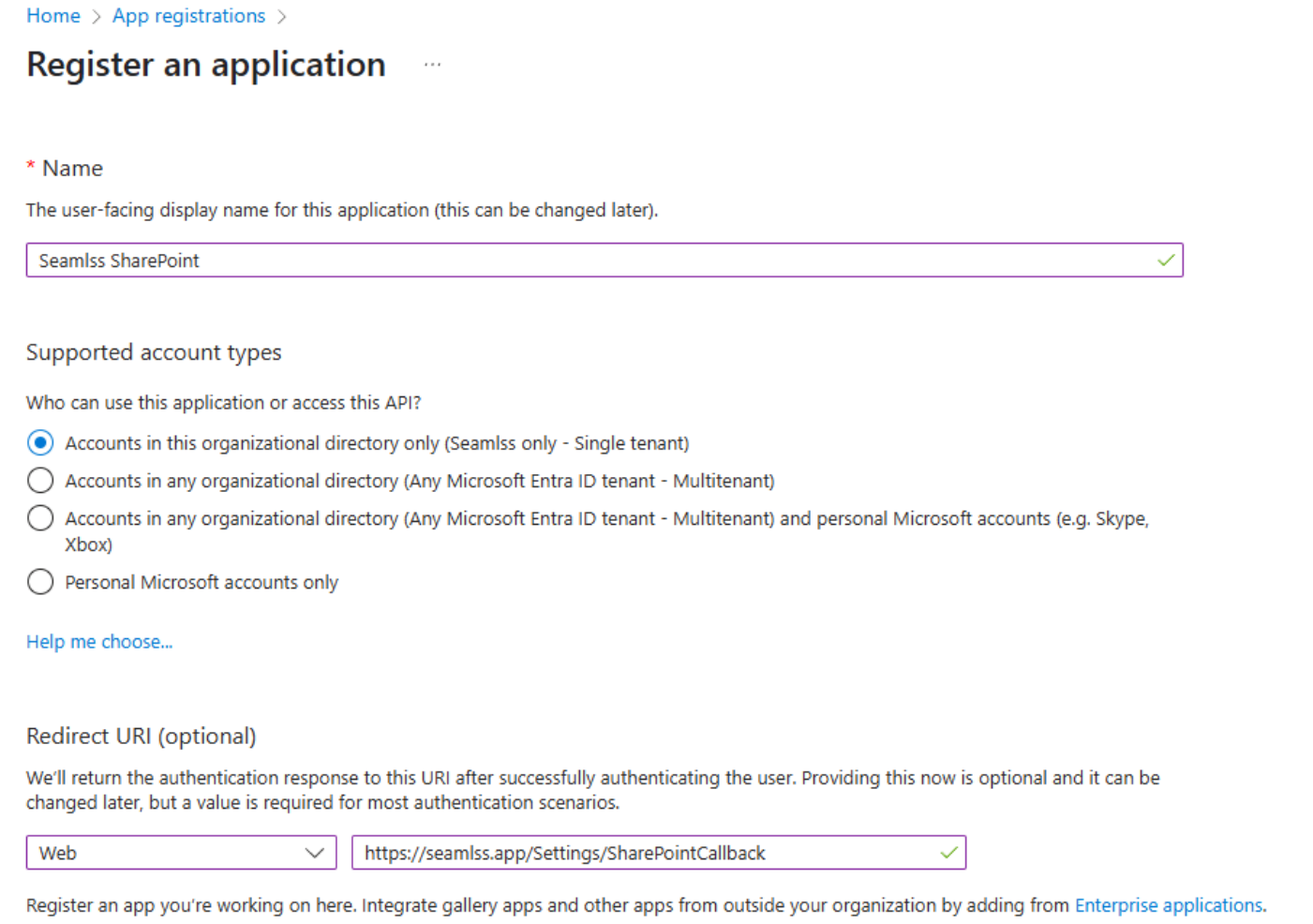
Integrated Apps · https://seamlss.com.au/help/sharepoint-integration-with-seamlss/

## Step 1: Create the App in Microsoft Entra

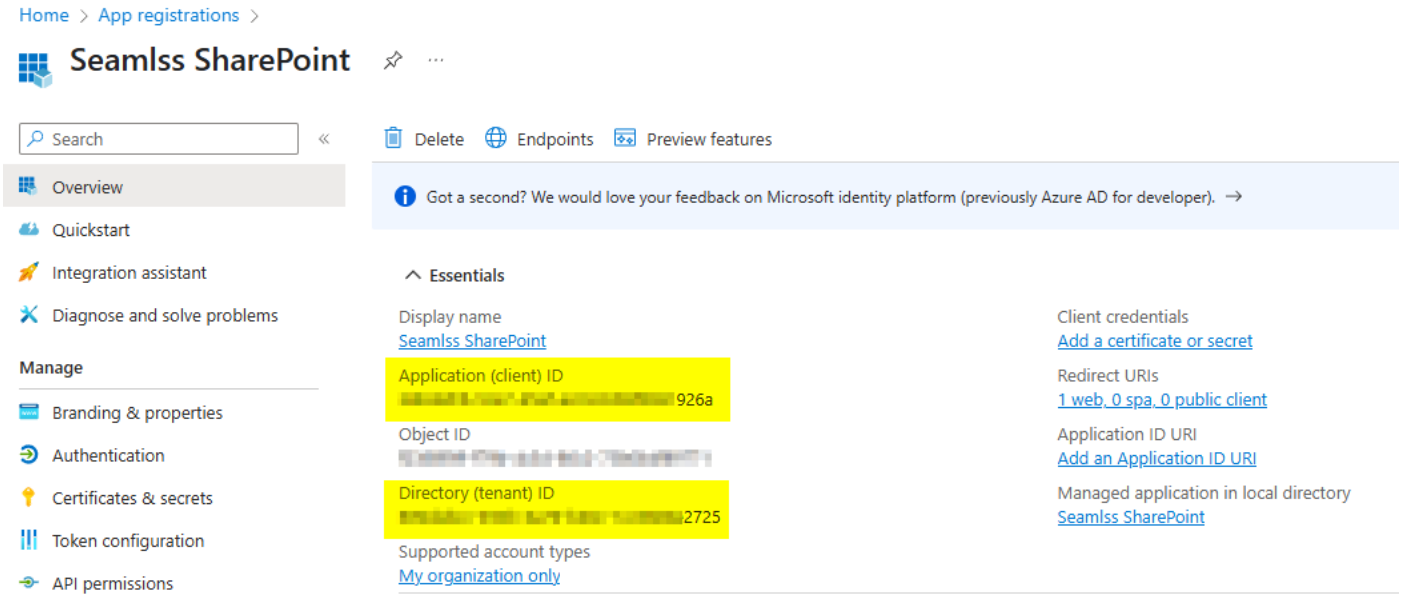
- Go to: Microsoft Entra App Registrations
- Login as MS Office 365 admin
- Click on **Applications > App registrations**: from the left hand menu, if not already selected.




- Click **“+ New registration”**
- Name: It can be anything, but we recommend, `Seamlss SharePoint`
- Supported account type: **Accounts in this organisational directory only (Single tenant)**
- Redirect URI:
  - Select **Web** from the dropdown
  - URI: `https://seamlss.app/Settings/SharePointCallback`
- Click **Register**
- dd

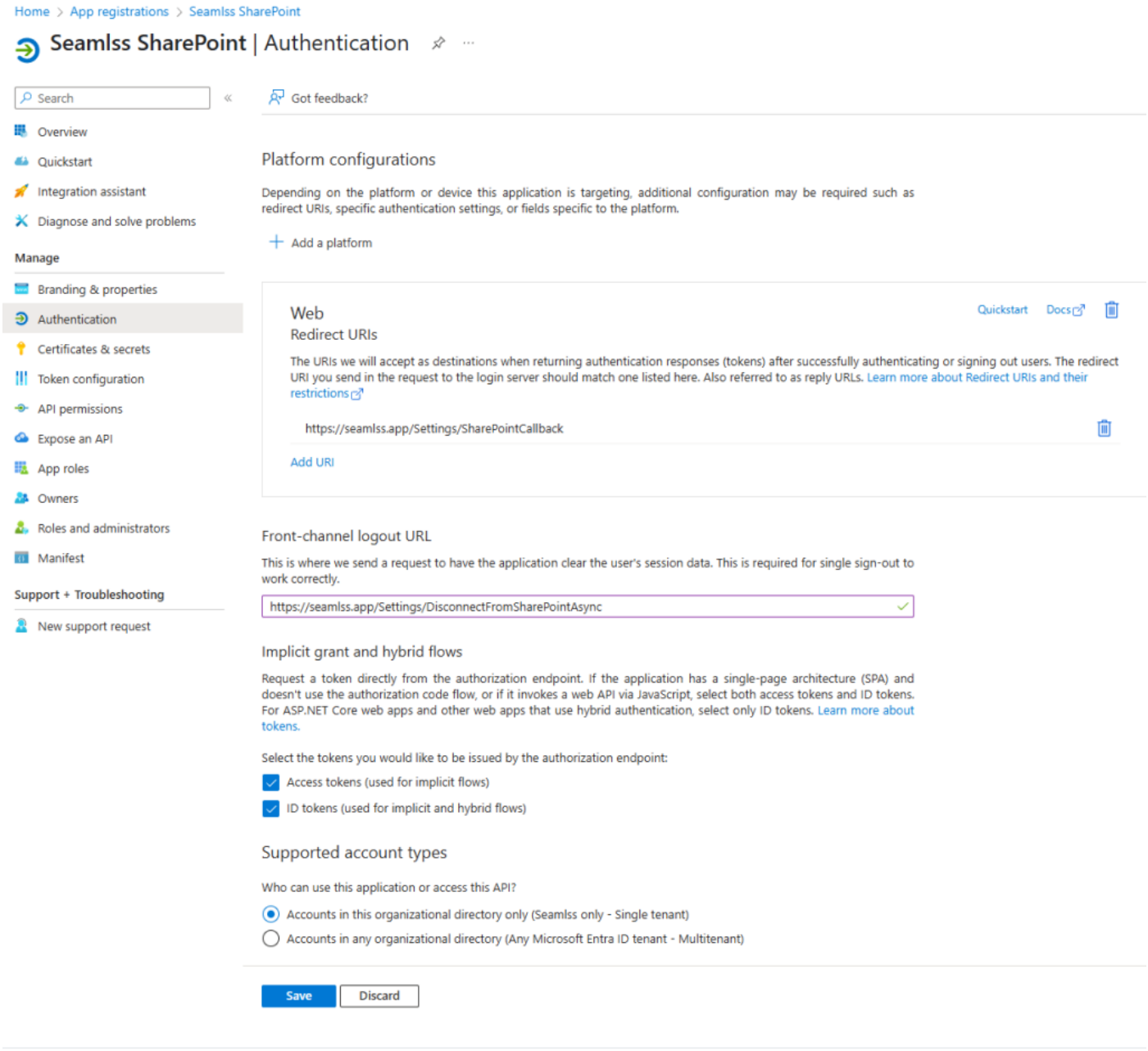



- Once completed, take note of the **Application (client) ID**, along with your **Directory (tenant) ID**. These will be used later.



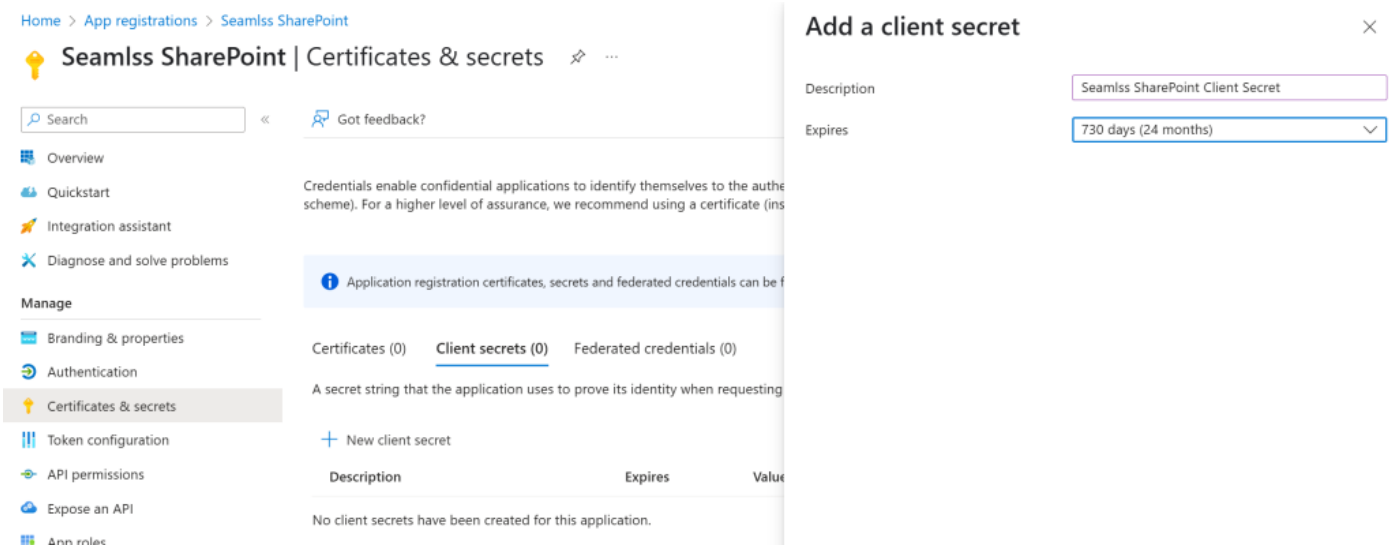
## Step 2: Configure Authentication Settings

- Go to the app's **Authentication** menu
- Confirm Web platform is configured correctly.
  - This should already be configured, but otherwise click "Add a platform", select "Web" and for Redirect URI enter: `https://seamlss.app/Settings/SharePointCallback`
- Set the following for **Front-channel logout URL:** `https://seamlss.app/Settings/DisconnectFromSharePointAsync`
- Under **Implicit grant and hybrid flows**, tick both boxes.
- Finally, for **Supported account types** select "Accounts in this organisational directory only ( _*Your org*_: Single tenant)".
- Leave Advanced settings as-is, and click **Save**



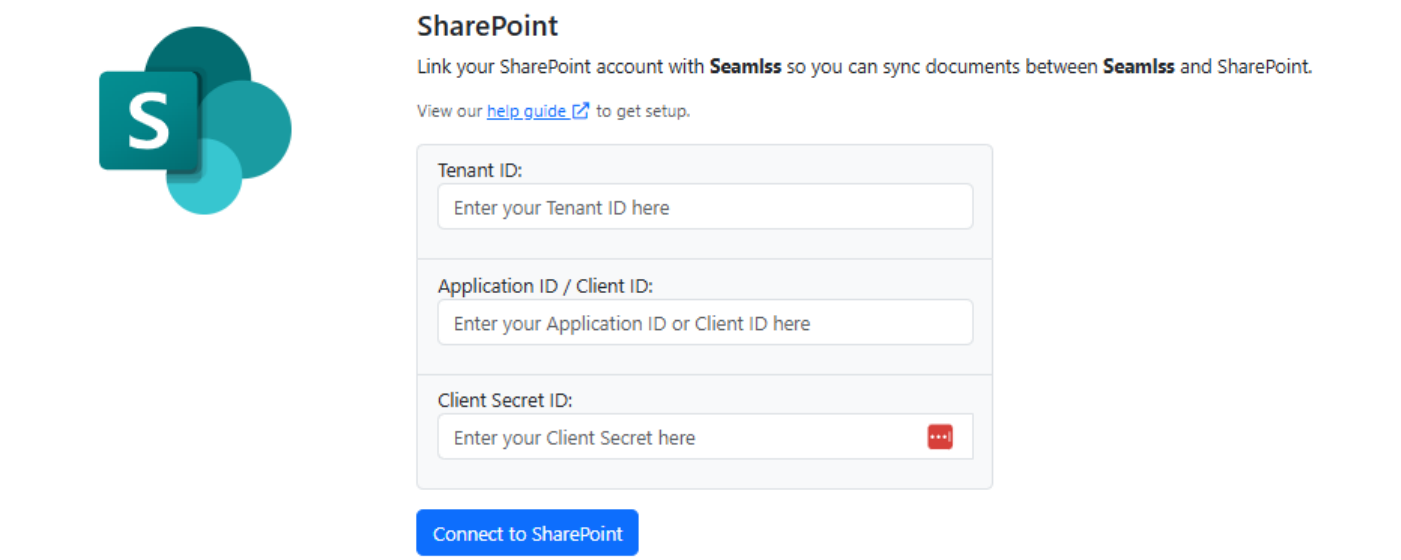

## Step 3: Generate a Client Secret

- Navigate to **Certificates & secrets**
- Under “Client secrets,” click **+ New client secret**
  - Description: `Seamlss SharePoint Client Secret`
  - Expiry: 6 to 24 months recommended
- Click **Add** and **copy the VALUE immediately** (you won’t be able to retrieve it again later)




Return to the **Seamlss SharePoint integration page** and paste the Client Secret into the Client Secret ID field. You can also copy and paste the Tenant ID and Application ID / Client ID at this stage if you like.

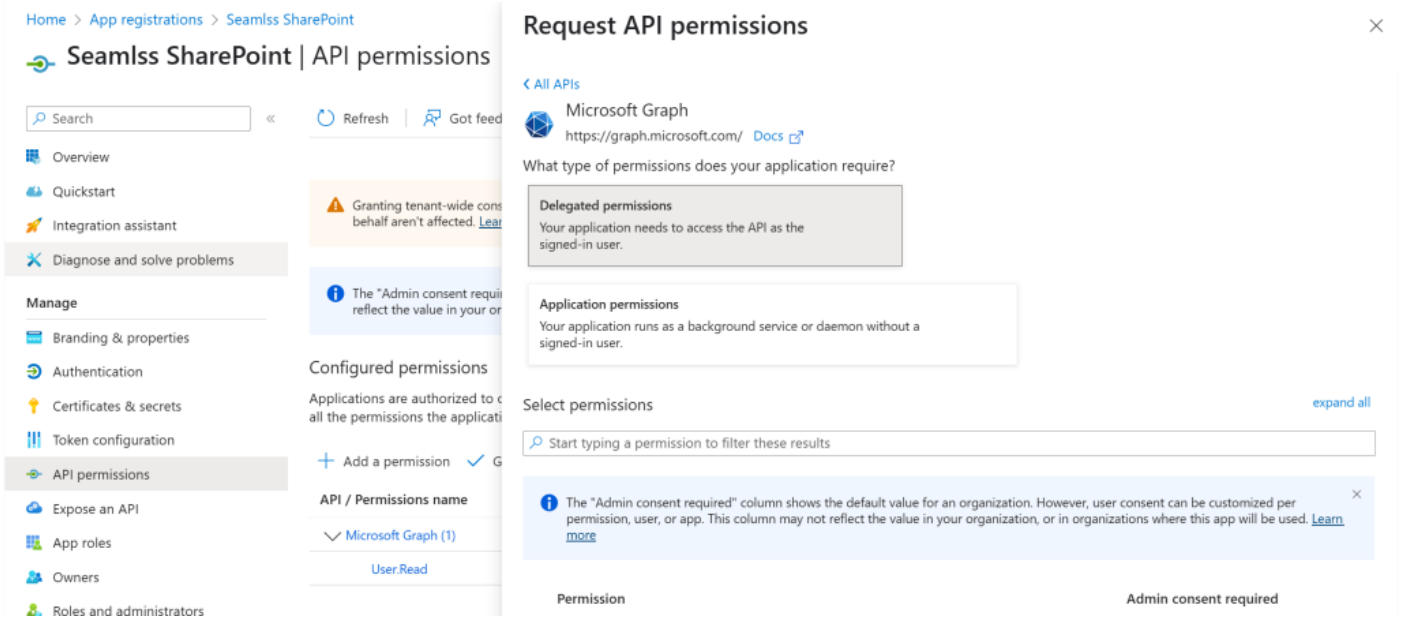
---




---

## Step 4: Add Delegated API Permissions

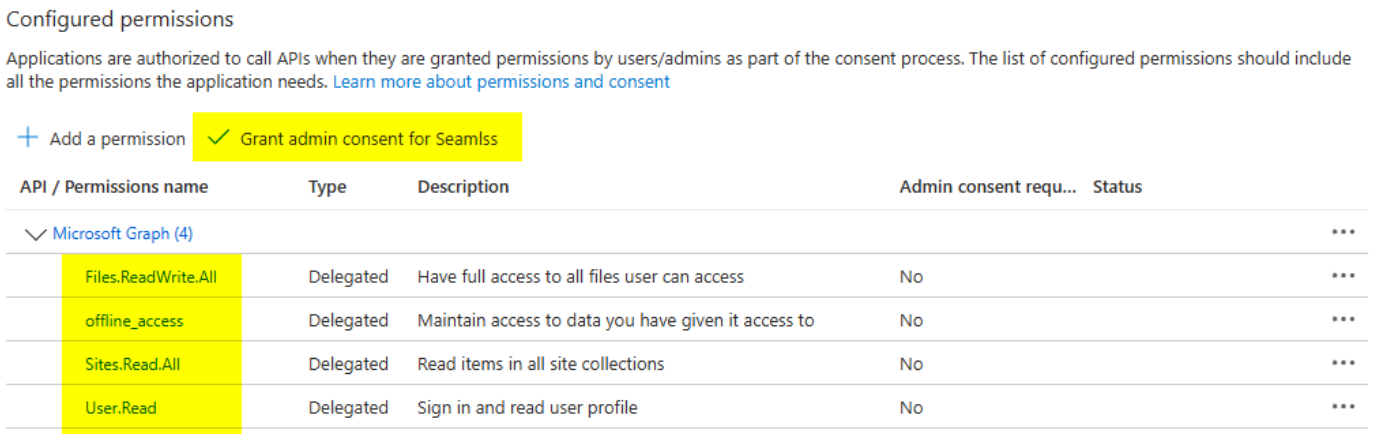
Go to **API Permissions > + Add a permission > Microsoft Graph > Delegated permissions**



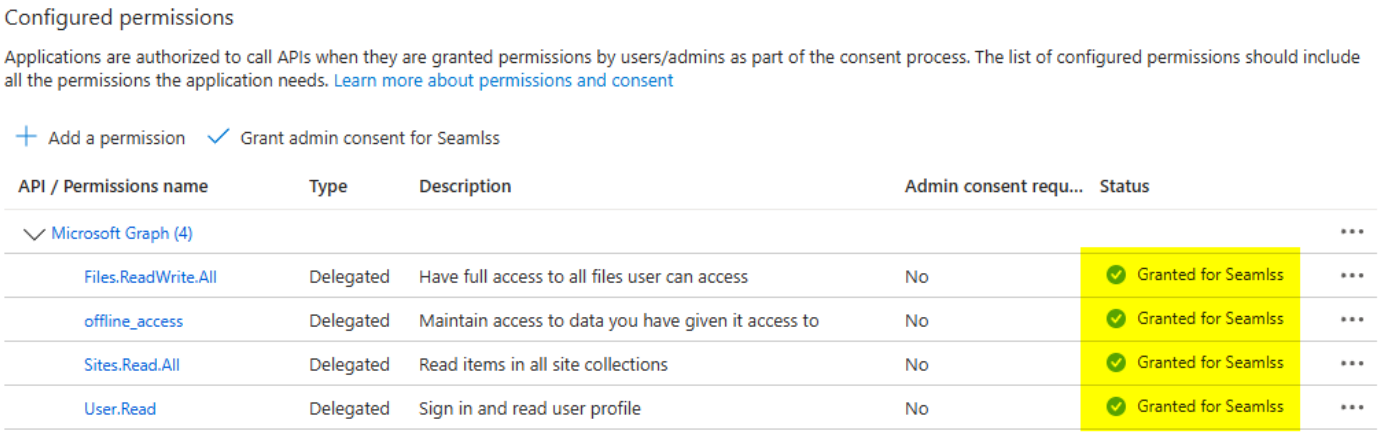

- Add the following: *(use the search bar to find them quickly and easily)*
  - `Files.ReadWrite.All`
  - `Sites.Read.All`
  - `offline_access`

You should see the permissions added like below (User.Read will already be added).

After adding the permissions, click **Grant admin consent**:

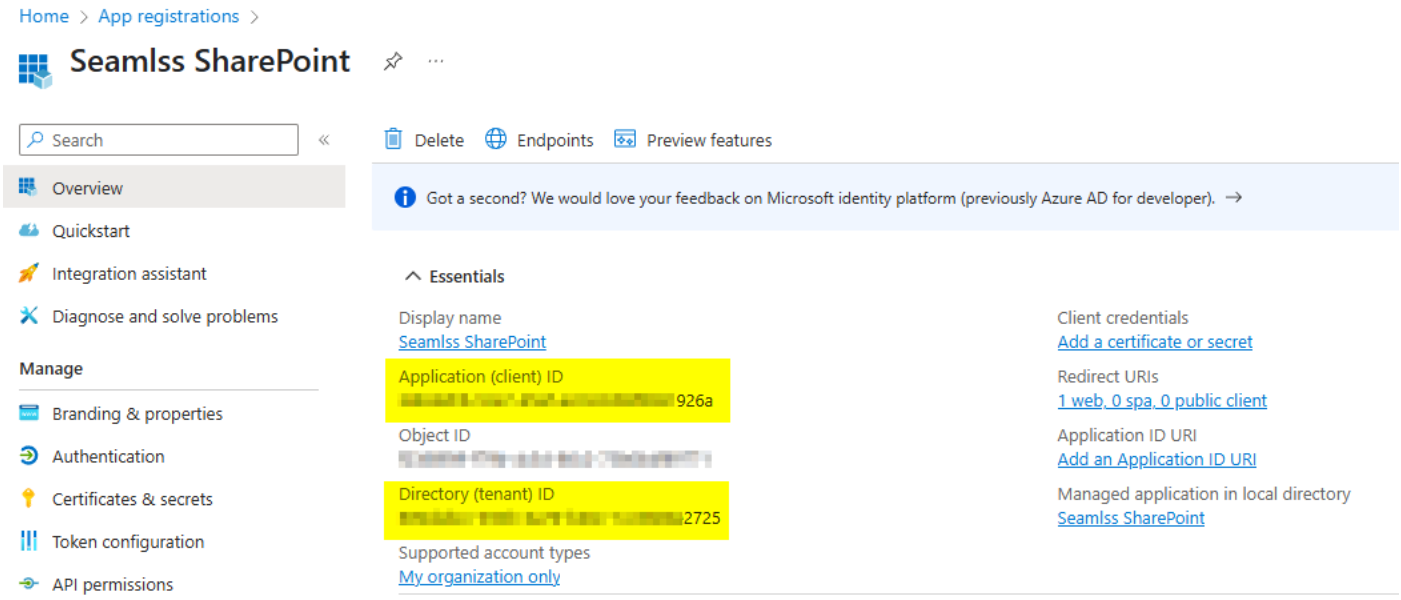



The Status should then say Granted for each permission. Your Application setup is now complete.



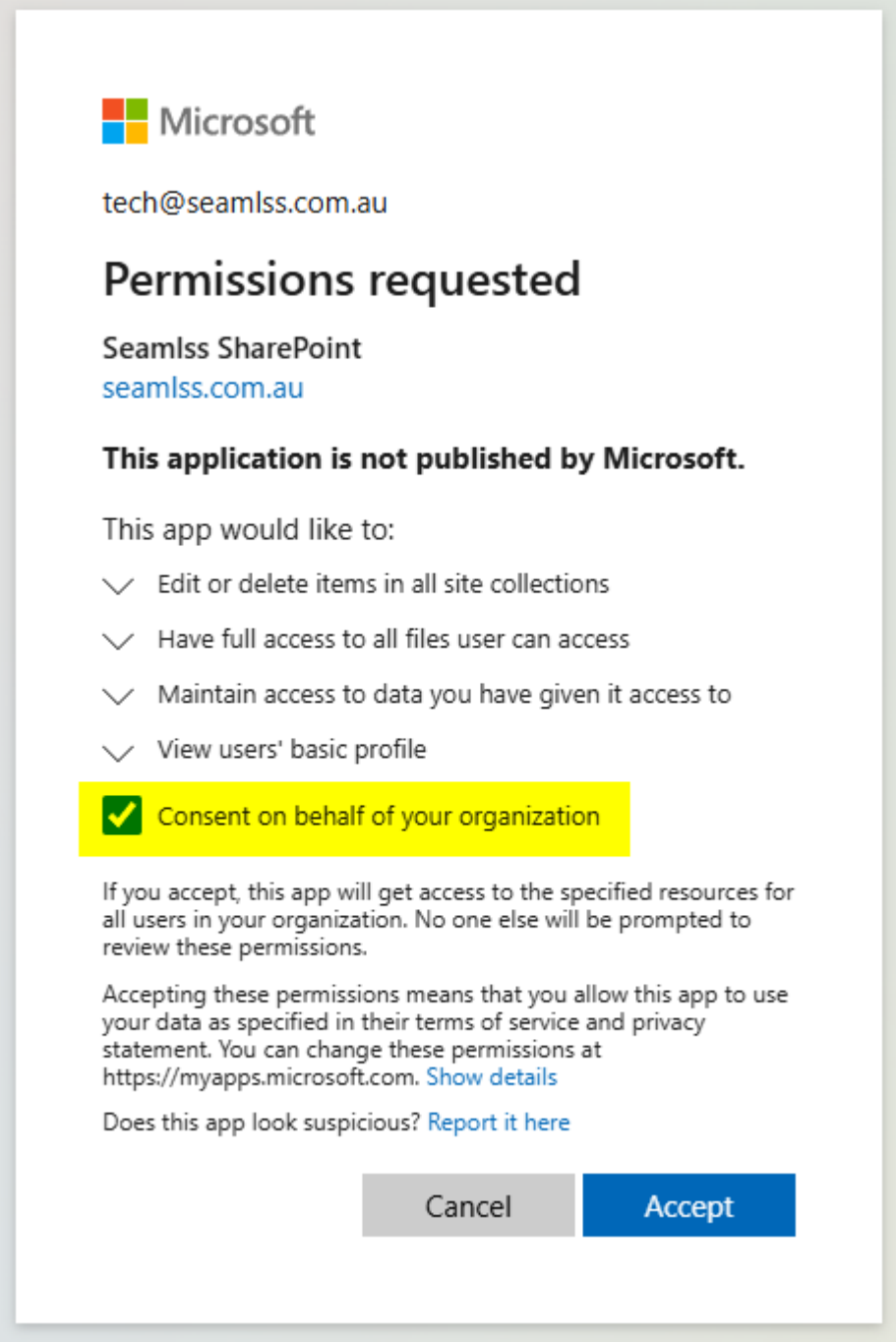

## Step 5: Connect in Seamlss

Return to the Overview menu to copy the required fields below.

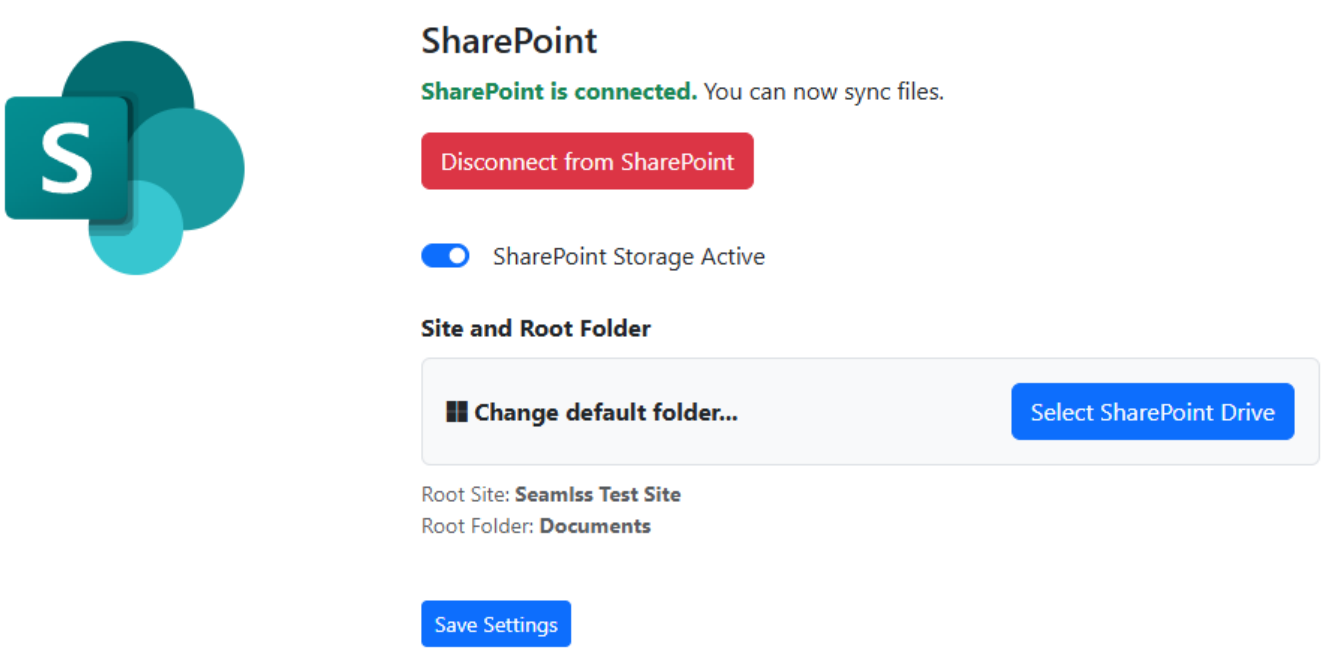



Now go to **Seamlss** to complete the connection:

- Go to the SharePoint integration setup section
- Enter the following values:
  - **Directory (tenant) ID** => Tenant ID
  - **Application (client) ID** => Application ID / Client ID
  - **Client Secret** => Client Secret ID (from Step 3) *if you didn't you will have to go back and create another*
- Click **Connect to SharePoint**, follow the prompts to sign in as admin, ensuring you tick the Consent box and Accept.




- Once authenticated, use the **Select SharePoint Drive** button to select a site and documents folder (e.g. Business Edge Accounting > Documents)
- Click the **Save Setting**s button to finish.




## Notes

- Connecting SharePoint will disconnect any previous OneDrive or Google Drive integration.
- The Microsoft Entra app must be registered under the **same tenant** as the user's Microsoft 365 account used for connection.
- Ensure "Web" is explicitly selected when entering Redirect URIs. This is easy to miss.

## Troubleshooting

### Redirect URI Mismatch

Ensure the redirect URI in Microsoft Entra exactly matches the one used by Seamlss:

- `https://seamlss.app/Settings/SharePointCallback`

If not, add it under **Authentication > Platform configurations** and save.

### Secret Errors

- Ensure the **secret value** is used (not the secret ID)
- If unsure, generate a new one and replace it in Seamlss

### Consent Issues

- Admins must click **Grant admin consent** in the Azure portal
- If it fails silently, confirm that each permission shows “Granted” next to it

### Login or Sync Fails

- Clear cookies or try an incognito window
- Ensure the user connecting via Seamlss belongs to the same Microsoft 365 tenant where the app was registered
- Refresh the client secret or tenant/client ID values in Seamlss if they’ve changed

### What Not to Do

- Don’t use **Application-type** permissions
- Don’t register the app as multi-tenant
- Don’t use wildcard (`*`) URIs
- Don’t forget to select “Web” when configuring Redirect URIs