# App Registration and Integration Setup for Microsoft Azure

## Table of Contents

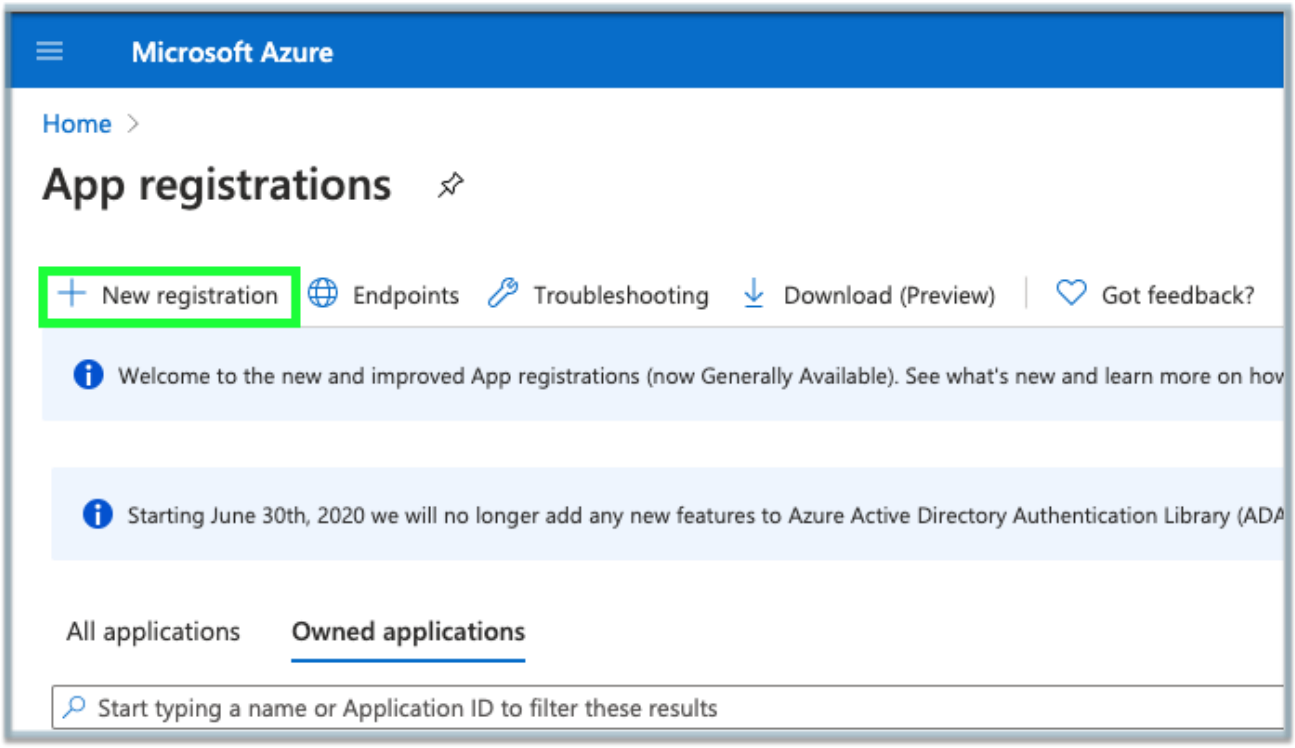
# 1. Password Reset for Azure

Espressive Barista has the ability to reset the password for Microsoft Azure users who have forgotten their password or do not have access to start with. In order to have this working for Azure Active Directory, some additional steps are needed.

## 1.1 Creating an App Registration

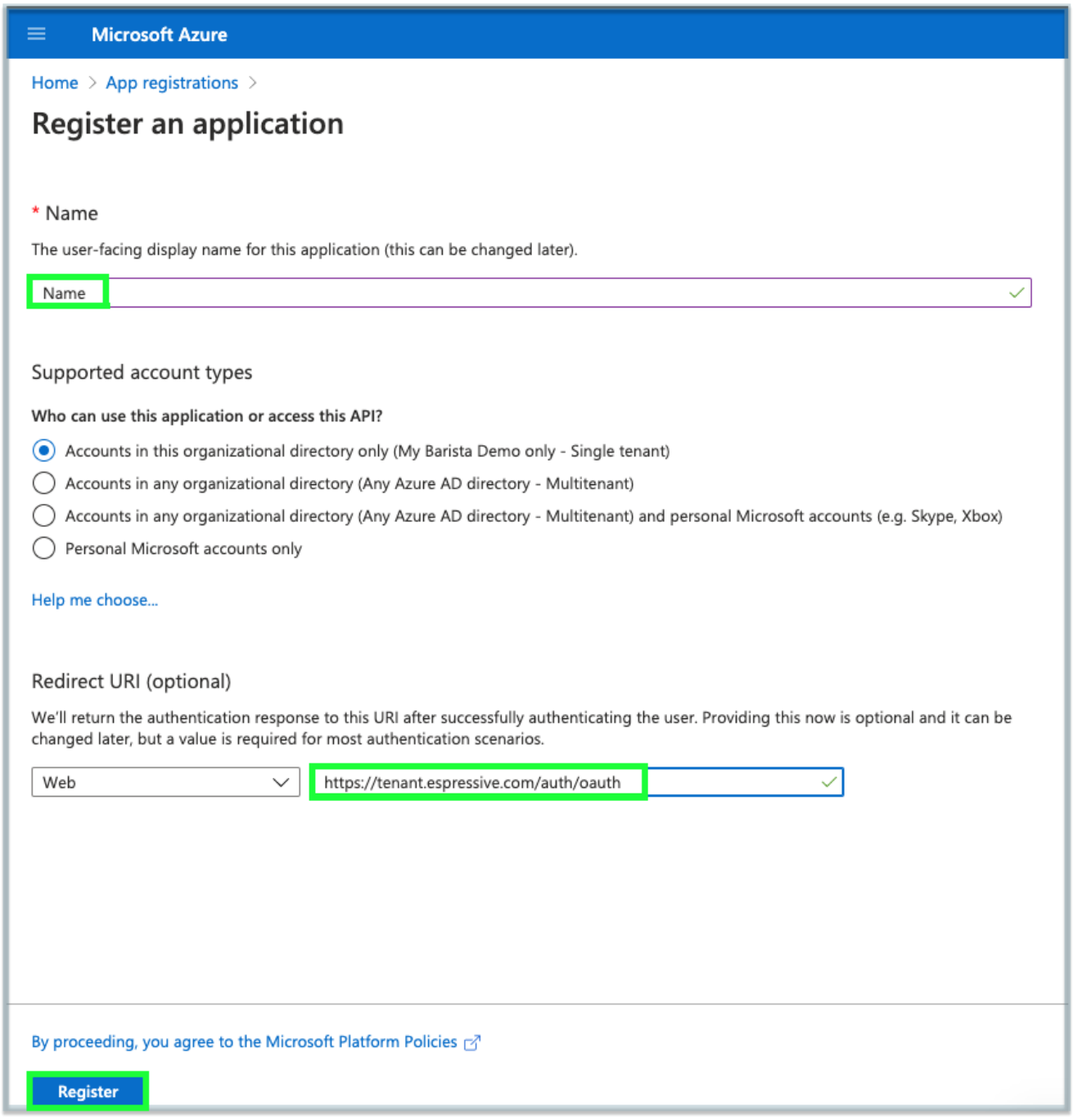
In order to connect your tenant to Active Directory, first create an app registration. If you already have one, you can skip these steps. Otherwise this can be done as follows:

1. Log in to Azure as ad admin user. Global Admin is always the preferable role.
2. Type **App registrations** into the search box.
3. Click on **App registrations**.
4. Click on **New registration**.



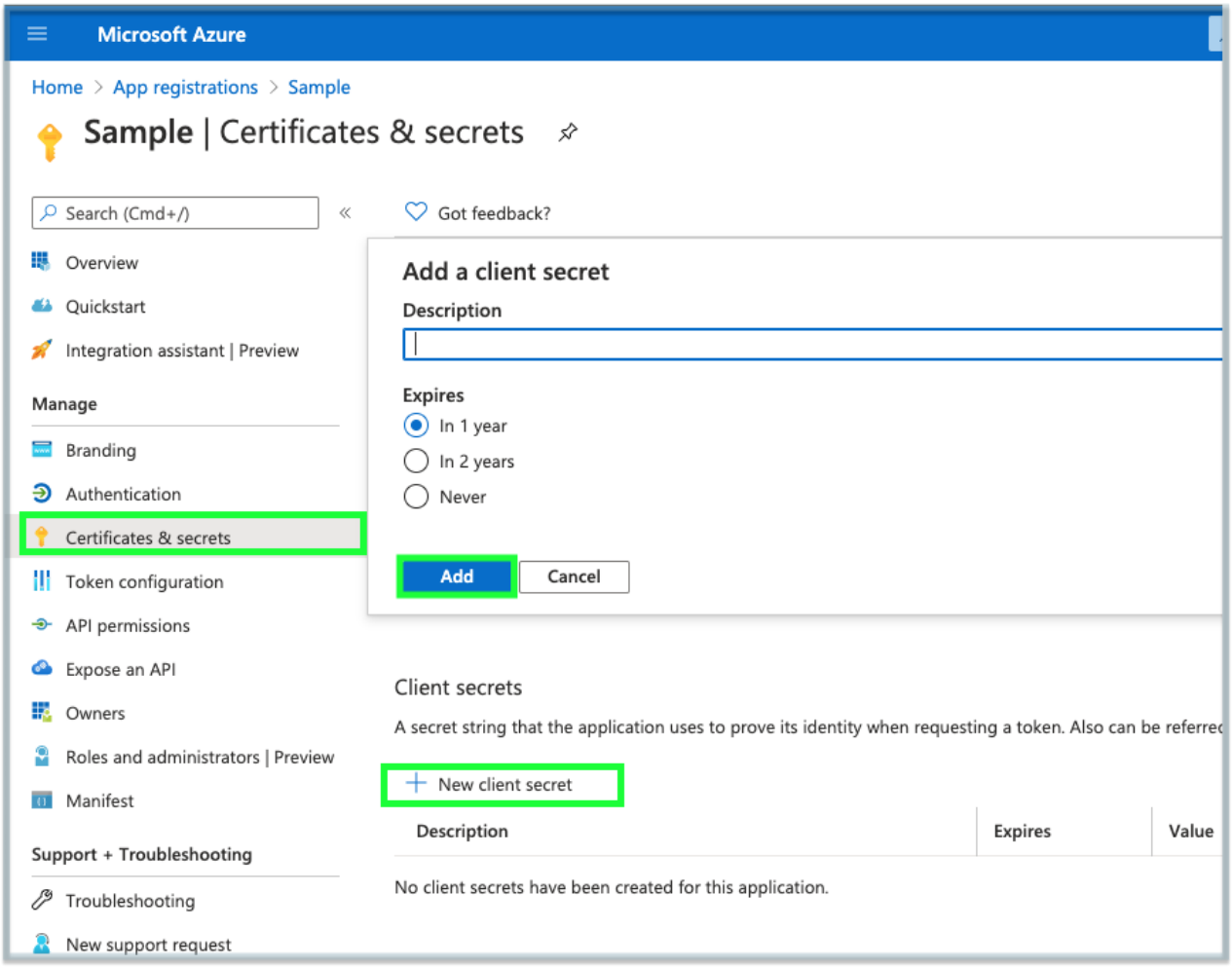

5. Provide a name for the registration, preferably something descriptive and unique.
6. In the **Redirect URL** section:
   6.1 Select Web option in the dropdown.
   6.2 In the text field, type: `https://{tenant}.espressive.com/auth/outh`

7. Click **Register**.




8. On the app registration page, click on **Certificates & secrets**.
9. Scroll down to the **Client Secrets** section.
10. Click on **New client secret**.

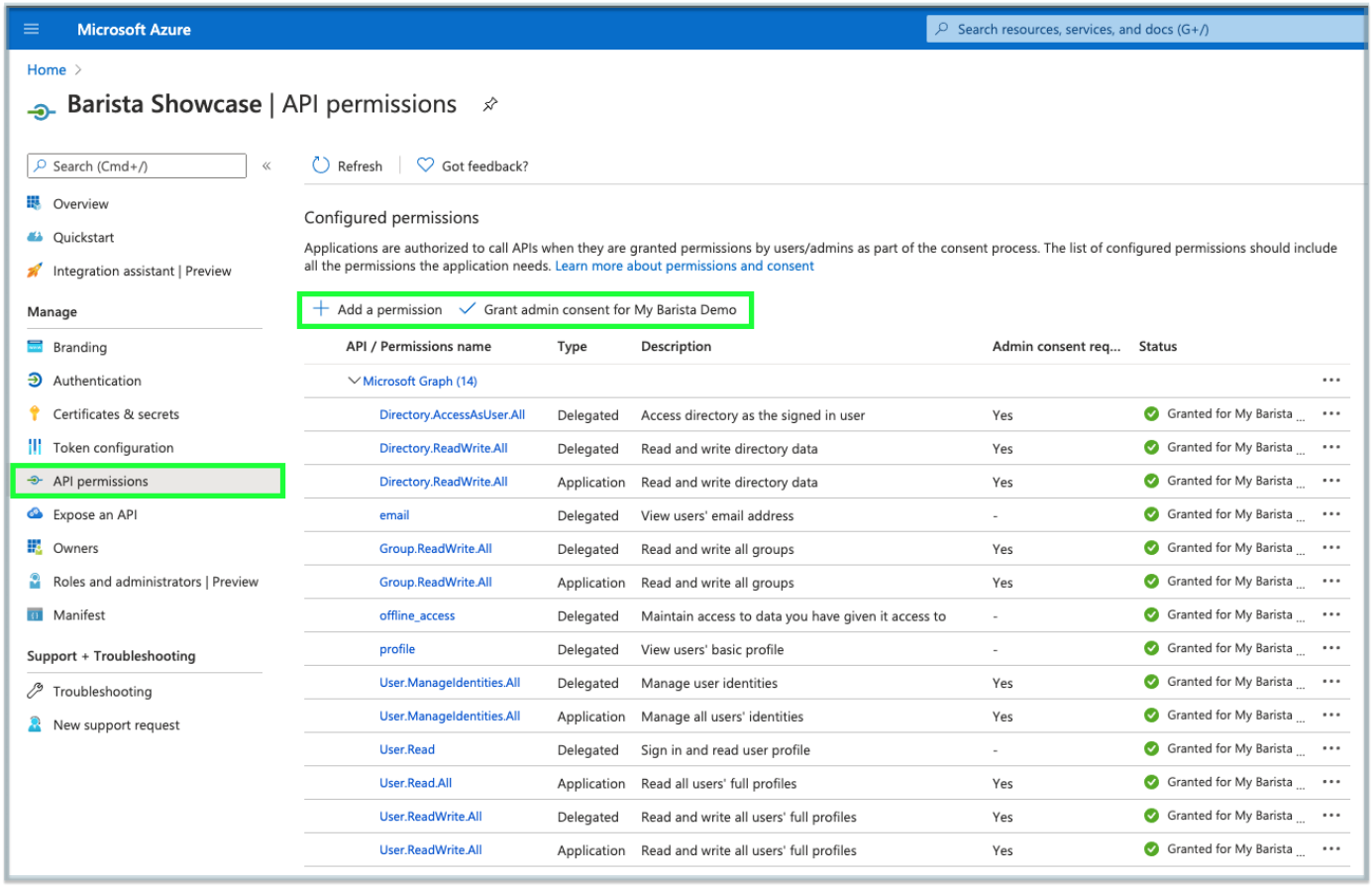
11. Provide a descriptive name for it and click **Add**.



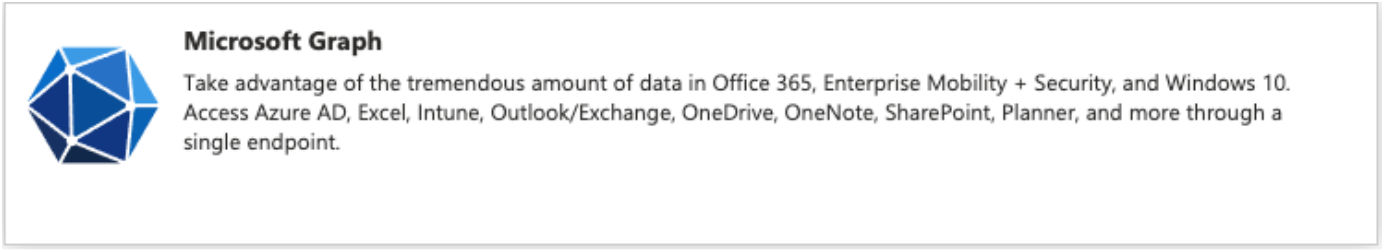

## 1.2 App Registration Permissions

Once an app registration is in place, you need to provide proper permissions in order to reset passwords.

1. Click on **API permissions**.
2. Click on **Add a permission**.




3. Click on **Microsoft Graph**.



4. Select the permissions listed in the table below.

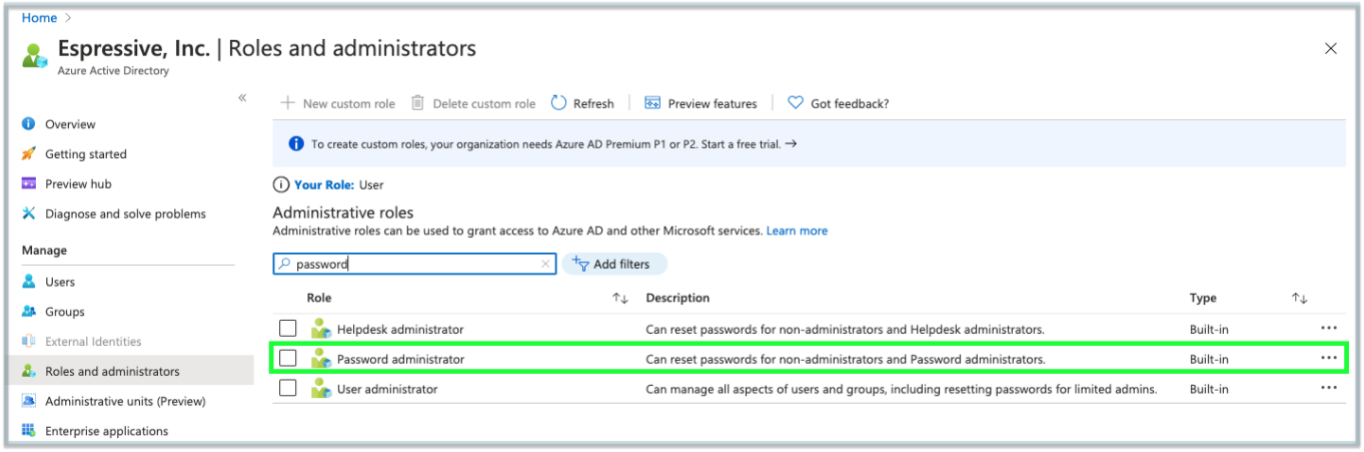
| Permission | Type | Description |
|---|---|---|
| Directory.AccessAsUser.All | Delegated | Access directory as the signed-in user |
| Directory.ReadWrite.All | Delegated | Read and write directory data |
| Directory.ReadWrite.All | Application | Read and write directory data |
| Email | Delegated | View a users' email address |
| Group.ReadWrite.All | Delegated | Read and write all groups |
| Group.ReadWrite.All | Application | Read and write all groups |
| offline_access | Delegated | Maintain access to data you have given it access to |
| Profile | Delegated | View a users' basic profile |
| User.ManageIdentities.All | Delegated | Manage user identities |
| User.ManageIdentities.All | Application | Manage all users' identities |
| User.Read | Delegated | Sign in and read user profile |
| User.Read.All | Application | Read all users' full profiles |
| User.ReadWrite.All | Delegated | Read and write all users' full profiles |
| User.ReadWrite.All | Application | Read and write all users' full profiles |

5. Click on **Grant admin consent for {tenant}**.

## 1.3 Assign Role

You need to assign the Password Administrator role to the User Principal associated with your app registration.

1. Go to the Azure Active Directory.
2. Click on **Roles and administrators** from the menu on the left.
3. Inside this section, search for “Password administrator.”
4. Click on the **Password administrator** option.



5. Click on **Add assignments**.
6. On the left side menu, search for your app registration name.
7. Select the app registration listed.
8. Click on **Add**.