

App Registration and Integration Setup for **Microsoft Azure**

Table of Contents

1. Password Reset for Azure	2
1.1 Creating an App Registration	2
1.2 App Registration Permissions	4
1.3 Assign Role	6

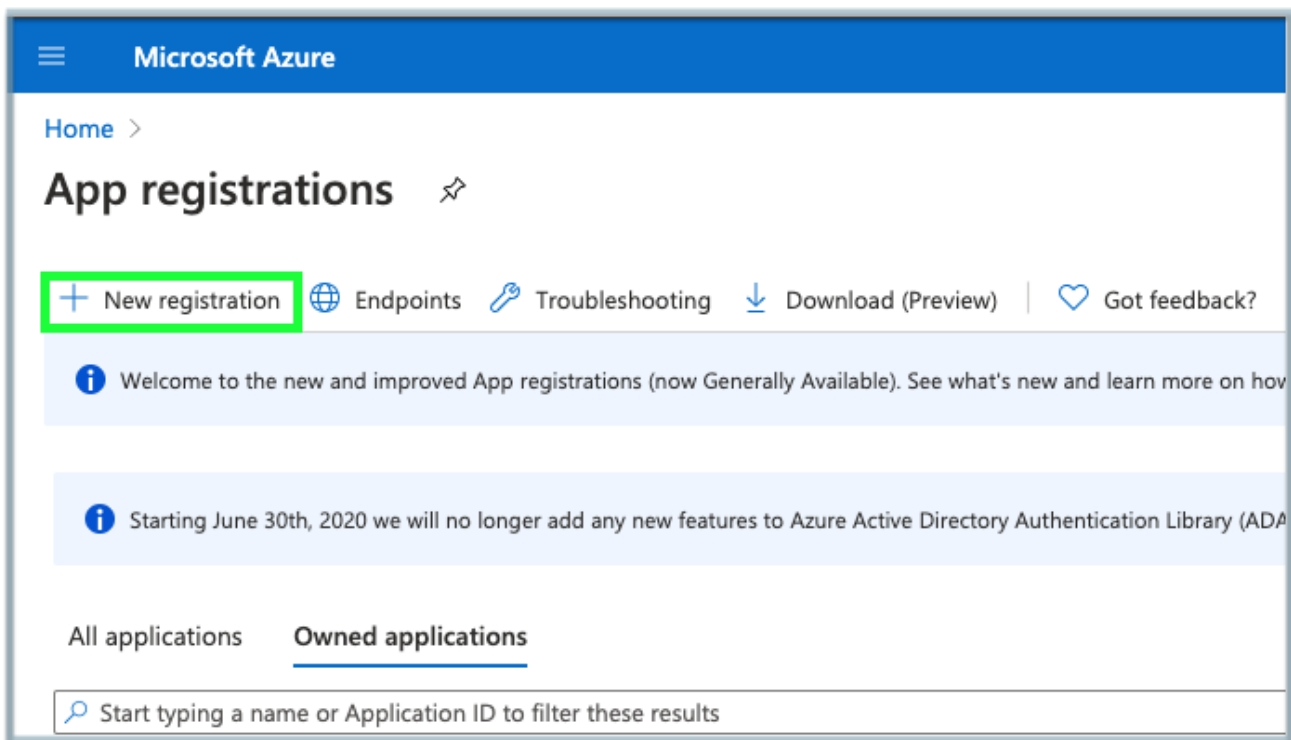
1. Password Reset for Azure

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**.

Microsoft Azure

Home > App registrations >

Register an application

*** Name**
The user-facing display name for this application (this can be changed later).

Name ✓

Supported account types

Who can use this application or access this API?

- Accounts in this organizational directory only (My Barista Demo 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.

Web ✓ ✓

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

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**.

The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes the Microsoft Azure logo and the breadcrumb path: Home > App registrations > Sample. The main heading is 'Sample | Certificates & secrets'. A search bar and a 'Got feedback?' link are visible. The left sidebar contains a navigation menu with categories: Overview, Quickstart, Integration assistant | Preview, Manage (with sub-items: Branding, Authentication, Certificates & secrets, Token configuration, API permissions, Expose an API, Owners, Roles and administrators | Preview, Manifest), and Support + Troubleshooting (with sub-items: Troubleshooting, New support request). The 'Certificates & secrets' item is highlighted with a green box. A modal dialog titled 'Add a client secret' is open, featuring a 'Description' text input field, an 'Expires' section with radio buttons for 'In 1 year' (selected), 'In 2 years', and 'Never', and 'Add' and 'Cancel' buttons. Below the dialog, the 'Client secrets' section is visible, with a '+ New client secret' button highlighted in green. A table with columns 'Description', 'Expires', and 'Value' is shown, but it is empty, with the message 'No client secrets have been created for this application.' below it.

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**.

The screenshot shows the Microsoft Azure portal interface for configuring API permissions for an application named 'Barista Showcase'. The left-hand navigation pane is visible, with 'API permissions' highlighted. The main content area shows a list of configured permissions under the 'Microsoft Graph' category. At the top of this list, there are two buttons: '+ Add a permission' and 'Grant admin consent for My Barista Demo', both of which are highlighted with a green border. Below these buttons is a table of permissions.

API / Permissions name	Type	Description	Admin consent req...	Status
Microsoft Graph (14)				
Directory.AccessAsUser.All	Delegated	Access directory as the signed in user	Yes	Granted for My Barista ...
Directory.ReadWrite.All	Delegated	Read and write directory data	Yes	Granted for My Barista ...
Directory.ReadWrite.All	Application	Read and write directory data	Yes	Granted for My Barista ...
email	Delegated	View users' email address	-	Granted for My Barista ...
Group.ReadWrite.All	Delegated	Read and write all groups	Yes	Granted for My Barista ...
Group.ReadWrite.All	Application	Read and write all groups	Yes	Granted for My Barista ...
offline_access	Delegated	Maintain access to data you have given it access to	-	Granted for My Barista ...
profile	Delegated	View users' basic profile	-	Granted for My Barista ...
User.ManageIdentities.All	Delegated	Manage user identities	Yes	Granted for My Barista ...
User.ManageIdentities.All	Application	Manage all users' identities	Yes	Granted for My Barista ...
User.Read	Delegated	Sign in and read user profile	-	Granted for My Barista ...
User.Read.All	Application	Read all users' full profiles	Yes	Granted for My Barista ...
User.ReadWrite.All	Delegated	Read and write all users' full profiles	Yes	Granted for My Barista ...
User.ReadWrite.All	Application	Read and write all users' full profiles	Yes	Granted for My Barista ...

3. Click on **Microsoft Graph**.

Microsoft Graph
 Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.

- 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

- 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.

- Go to the [Azure Active Directory](#).
- Click on **Roles and administrators** from the menu on the left.
- Inside this section, search for "Password administrator."
- Click on the **Password administrator** option.

The screenshot shows the Azure Active Directory interface for 'Espressive, Inc. | Roles and administrators'. A search bar contains the text 'password'. Below the search bar, a table lists the following roles:

Role	Description	Type
<input type="checkbox"/> Helpdesk administrator	Can reset passwords for non-administrators and Helpdesk administrators.	Built-in
<input type="checkbox"/> Password administrator	Can reset passwords for non-administrators and Password administrators.	Built-in
<input type="checkbox"/> User administrator	Can manage all aspects of users and groups, including resetting passwords for limited admins.	Built-in

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**.

