

Working with Espressive Barista and Microsoft Azure

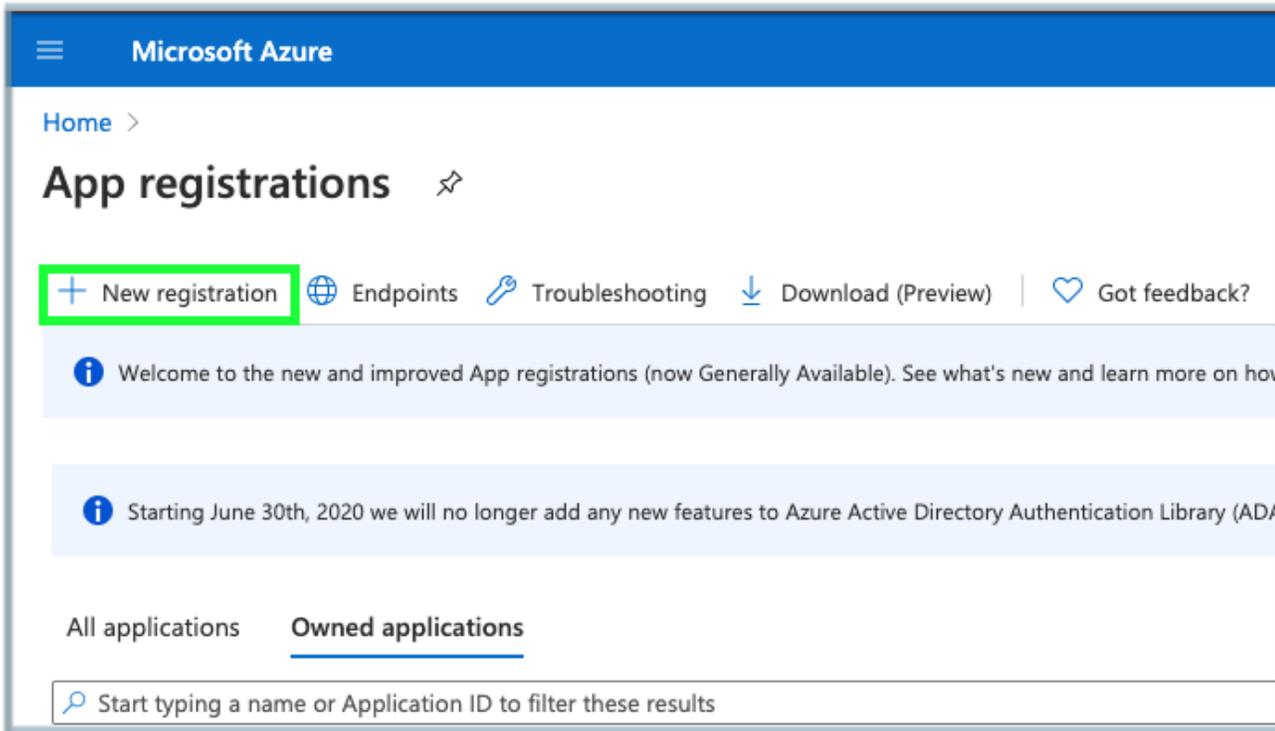
Password Reset for Azure

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

Creating an App Registration

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

1. Log in to [Azure](#) as an admin user. Global Admin is always a preferable role.
2. Type **App Registrations** into the search box.
3. Click on **App Registrations**.
4. Click on **New Registrations**.



5. Provide a name for the registration, preferably 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 ▼ https://tenant.espressive.com/auth/oauth ✓

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 is blue with the 'Microsoft Azure' logo. Below it, the breadcrumb trail reads '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 'Manage' section with 'Certificates & secrets' highlighted in green. The main content area shows a modal dialog titled 'Add a client secret'. The dialog has a 'Description' text field, 'Expires' radio buttons (with 'In 1 year' selected), 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.'

App Registration Permissions

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

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

Microsoft Azure

Home > Barista Showcase | API permissions

Search (Cmd+/) Refresh Got feedback?

Overview
Quickstart
Integration assistant | Preview

Manage

Branding
Authentication
Certificates & secrets
Token configuration
API permissions
Expose an API
Owners
Roles and administrators | Preview
Manifest

Support + Troubleshooting
Troubleshooting
New support request

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 My Barista Demo

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.

4. Select the permissions listed in the table below.

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

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 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 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

Assign Role

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

1. Go to [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.

The screenshot shows the 'Roles and administrators' page in the Azure Active Directory portal. The search bar contains the text 'password'. The results table is as follows:

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**.

Add assignments ✕

Search ⓘ

 ✕

BM Barista Mocha
barista.mocha@espressivo.com

- Mocha
XXXXXXXXXX@XXXXXXXXXX
- Mocha Test Karthik
XXXXXXXXXX@XXXXXXXXXX

Selected items

No items selected

Add