

# Microsoft EWS Basic Authentication Migration

## Table of Contents

<a href="#">1. Overview</a> .....	2
<a href="#">2. Register Your Application</a> .....	2
<a href="#">3. Configure for Delegated Authentication and App-Only Authentication</a> .....	4
<a href="#">4. API Permissions</a> .....	5
<a href="#">5. Configure on the Espressive Barista App</a> .....	6

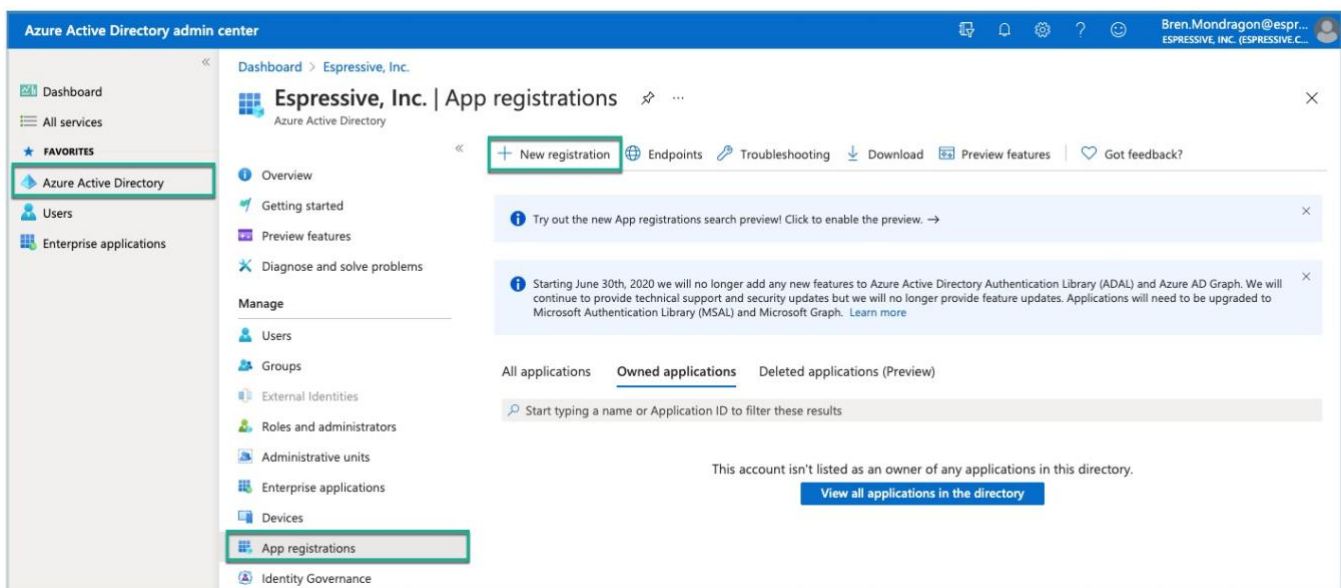
## 1. Overview

Currently, we use Microsoft Exchange Web Services (EWS) to access information in Office 365, specifically through Microsoft Graph for our Espressive Barista email integration. Recently [Microsoft deprecated the basic authentication protocol](#), so we now use the OAuth 2.0 protocol for authentication and authorization as a more secure way of connecting. This improvement in our authentication system also comes with a new user interface for the email integration available in our Barista admin tool. To proceed with the new changes, it is necessary to follow the steps of this document.

## 2. Register Your Application

To register your application:

1. Open your browser and navigate to the [Azure Active Directory admin center](#). Login using a **personal account** (i.e., Microsoft account).
2. Select **Azure Active Directory** in the left-hand navigation, then select **App registrations** under **Manage**.
3. Select **New registration**.



- Set **Name** to a friendly name for your app.
- Set **Supported account types** to the choice that makes sense for your scenario.
- For **Redirect URL**, change the dropdown to **Public client (mobile & desktop)** and set the value to:  
`urn:ietf:wg:oauth:2.0:oob`

4. Choose **Register**.

⚠ On the next page, copy the values of the **Application (client) ID** and **Directory (tenant) ID** and save them. You will need them for later.

Azure Active Directory admin center

Dashboard > Espressive >

## Register an application

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

Demo Espressive Customer X OAuth Integration

Supported account types

Who can use this application or access this API?

Accounts in this organizational directory only (Espressive 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 ... | urn:ietf:wg:oauth:2.0:oob

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

### 3. Configure for Delegated Authentication and App-Only Authentication

To use application permissions, follow these additional steps:

1. Select **Manifest** in the left-hand navigation under **Manage**.
2. Locate the `requiredResourceAccess` property in the manifest. Add the following inside the square brackets ( [ ] ):

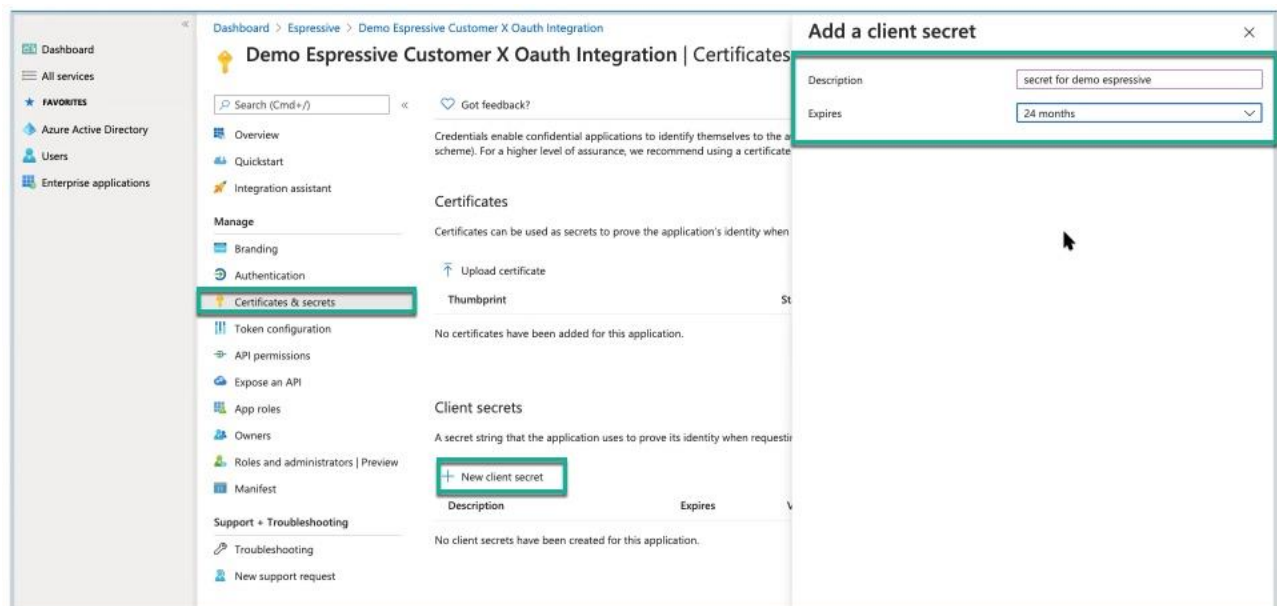
```

1 {
2   "resourceAppId": "00000002-0000-0ff1-ce00-000000000000",
3   "resourceAccess": [
4     {
5       "id": "3b5f3d61-589b-4a3c-a359-5dd4b5ee5bd5",
6       "type": "Scope"
7     },
8     {
9       "id": "dc890d15-9560-4a4c-9b7f-a736ec74ec40",
10      "type": "Role"
11    }
12  ]
13 }

```

3. Select **Save**.
4. Select **API permissions** under **Manage**.
5. Confirm that the `full_access_as_app` permission is listed.
6. Confirm that `EWS.AccessAsUser.All` permission is listed.
7. Select **Grant admin consent for org** and accept the content dialog.
8. Select **Certificates & secrets** in the left-hand navigation under **Manage**.
9. Select **New client secret**, enter a short description, and select **Add**.

⚠ Copy the **Value** of a newly added client secret and save it. You will need it later and you can only see it once.



## 4. API Permissions

1. Select **Azure Active Directory** in the left-hand navigation, then select **App registrations** under **Manage**.
2. Select your recently created application.
3. Select **API permissions** in the left-hand navigation under **Manage**.
4. Click on **Microsoft Graph**.
5. Enable **email**, **offline\_access**, **openid**, and **profile**.
6. Click on the **Update permissions** button.

Make sure you have all the permissions of this example image:

The screenshot shows the 'API permissions' page in the Azure Active Directory portal. The page title is 'Espressive Exchange OAUTH Test | API permissions'. The left-hand navigation menu is visible, with 'API permissions' selected. The main content area shows a table of configured permissions. The table has columns for 'API / Permissions name', 'Type', 'Description', 'Admin consent req...', and 'Status'. The permissions listed are:

API / Permissions name	Type	Description	Admin consent req...	Status
Microsoft Graph (5)				
email	Delegated	View users' email address	No	Granted for Espressive
offline_access	Delegated	Maintain access to data you have given it access to	No	Granted for Espressive
openid	Delegated	Sign users in	No	Granted for Espressive
profile	Delegated	View users' basic profile	No	Granted for Espressive
User.Read	Delegated	Sign in and read user profile	No	Granted for Espressive
Office 365 Exchange Online (2)				
EWS.AccessAsUser.All	Delegated	Access mailboxes as the signed-in user via Exchange W...	No	Granted for Espressive
full_access_as_app	Application	Use Exchange Web Services with full access to all mailb...	Yes	Granted for Espressive

Below the table, there is a note: 'To view and manage permissions and user consent, try Enterprise applications.'

## 5. Configure on the Espressive Barista App

1. Open your browser and login to your Barista environment: `https://<TENANT>.espressive.com/`
2. Select **More** from the left-hand menu, then select **Admin**.
3. Select **Integrations** from the menu and then select **Email**.
4. On the **Connections** drop-down menu, select "Microsoft Exchange OAuth."
5. Add an **Email Address** and **Name**.
6. Fill out the form using the **Application (client) ID**, **Directory (tenant) ID**, and the **Value** of the client secret you saved from before.
7. Click on the **TEST** button.
8. Click on **SAVE CHANGES**.

**Integrations** > Email

**Primary Email Account** | Barista Inboxes

**Connection**

Microsoft Exchange OAuth

**Name \***

Exchange Connection

**Email \***

xxxxx.sxxxxxxxx@xxxxxxxxxxxxx.com

**App ID**

xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx

**Tenant ID**

xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx

**Client Secret**

.....

Use this email account as a Barista Inbox

Check this box to use this account as an inbox for creating new requests. If you prefer to use a separate email account for Barista Inbox, click the "Barista Inboxes" tab at the top of this page.