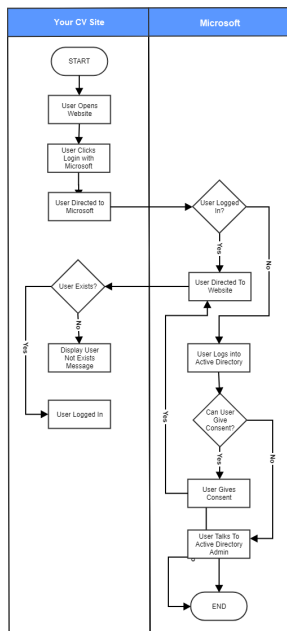


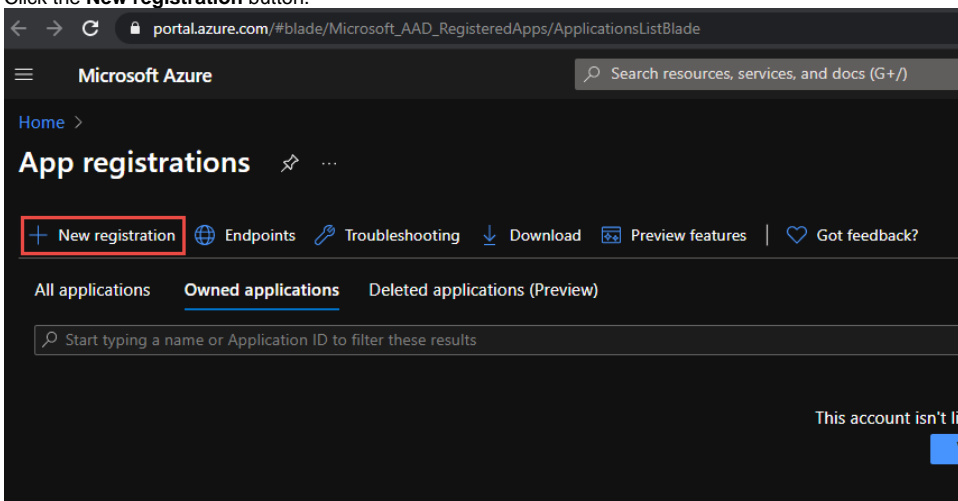
MS Active Directory Setup Guide

Integration Flowchart



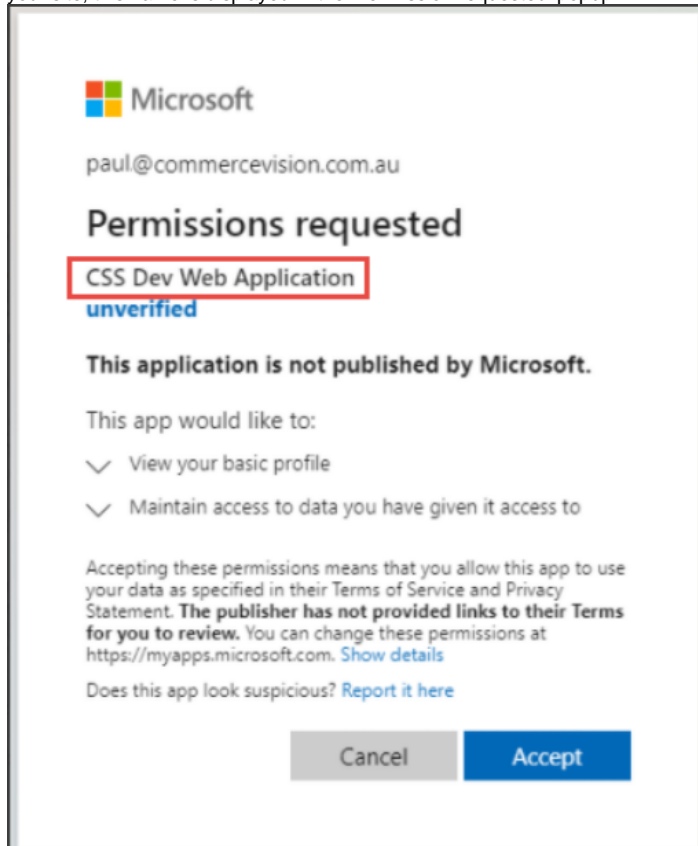
Register the Web App in Azure Portal

1. Login to your Azure Portal. If you have multi Active Directories in the Azure Portal, check you're on the correct Azure AD.
2. Navigate to the Microsoft identity platform for developers [App registrations](#) page.
3. Click the **New registration** button.

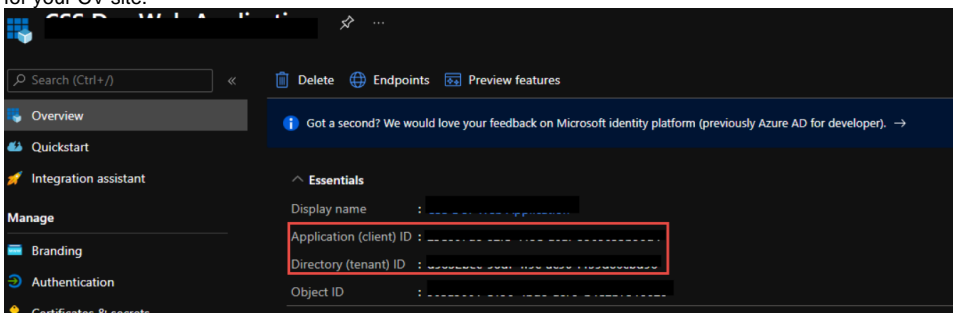


4. In the **Register an application page**, enter your application's registration information:

- a. In the **Name** section, enter a meaningful application name. **NOTE** - The first time a user selects to login with their Microsoft account on your site, this name is displayed in the 'Permission requested' popup.



5. Set the **Supported account types** as required:
1. **Accounts in this organizational directory only (Your Directory only - Single tenant)**
Only user and guest accounts in your directory can log in.
Use this option if your target audience is internal to your organization.
 2. **Accounts in any organizational directory (Any Azure AD directory - Multitenant)**
All users with a work/school account from Microsoft can log in. They include school/business Office 365 users.
Use this option if your target audience is business or educational customers and to enable multitenancy.
 3. **Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)**
All users with a work/school or personal Microsoft accounts can use your application or API. They include Office 365 schools/business users as well as personal accounts for services like Xbox and Skype.
Use this option to target the widest set of Microsoft identities and to enable multitenancy.
 4. **Personal Microsoft accounts only**
Personal accounts that are used to sign in to services like Xbox and Skype.
Use this option to target the widest set of Microsoft identities.
6. Set the redirect uri as your website url.
7. To create the application, click the **Register** button.
8. In the app's registration screen, make note of the **Application (client) ID** value and **Directory (tenant) ID** as these need to be entered in the CMS for your CV site.




9. In the app's registration screen, click on the **Authentication** tab in the left.


- a. In the Redirect URIs section, select **Web** and click **Add URI**.
 - b. Enter each of the following URIs separately, clicking 'add uri' each time.
 - <https://yourdomain.com/post.aspx>
 - <https://yourdomain.com/login.aspx>
 - <https://yourdomain.com>
 - c. In Front-channel logout URL, enter <https://yourdomain/signout-oidc>
 - d. In the **Advanced settings** | **Implicit grant** section, check **ID tokens**
 - e. **Supported account types** should already be selected correctly but change if required.
10. Click the **Save** button.
11. In the app's registration screen, click on the **Certificates & secrets** blade.
- a. In the **Client secrets** section, click on **New client secret**:
 - b. Type in the name: SingleSignOnClientSecret
 - c. Select one of the available key durations (**In 1 year**, **In 2 years**, or **Never Expires**) as per your security concerns.
 - d. To generate the key value, click the **Add** button.
 - e. Copy the generated value. **IMPORTANT** - This key value will not be displayed again, and is not retrievable by any other means. So make sure to note it down from the Azure portal before navigating to any other screen or blade.
12. To set up branding for the Permission Requested popup, click the **Branding** blade.
- a. Update all fields on this page and upload a brand logo.
 - b. If you have a Microsoft Partner Center (MPN) ID, add it here.
 - c. Click the **Save** button.

Now you can go into the CMS for your CV site and [configure the settings](#) for Active Directory SSO.

User Information

- The user must exist on the website where the email address matches the Microsoft Account email address. If this is not the case, the user will see the following error (N.B This can be configured in CMS - Third Party Login Features - Invalid User Message):

 **Login**
Please login to continue.

 Unable to login, your Microsoft account is not associated with a User.

Login with a social network

 Sign in with Microsoft

- The user must give the application permission (see Permission requested below) or the following error will be displayed. **NOTE** - This can be configured in CMS - Third Party Login Features - Declined Consent Message.



paul@commercevision.com.au

Permissions requested



CSS Dev Web Application
commercevision.com.au

This application is not published by Microsoft.

This app would like to:

- ✓ View your basic profile
- ✓ Maintain access to data you have given it access to

Accepting these permissions means that you allow this app to use your data as specified in their Terms of Service and Privacy Statement. You can change these permissions at <https://myapps.microsoft.com>. [Show details](#)

Does this app look suspicious? [Report it here](#)

Cancel

Accept

- A user can revoke the permission for the app from their Office 365 portal.



Login

Please login to continue.



Login failed as consent was declined.

Login with a social network



Sign in with Microsoft

Related help

- [Microsoft Azure AD SSO](#)