# Deskpro

## Creating an OAuth2 application in Office365

Phil Rigby - 2022-05-13 - Comment (1) - Legacy: Managing Deskpro On-Premise

To begin,  you will need to login to your **Azure Active Directory admin center**. If you're not sure how to get to this, it is possible to access it from your **Microsoft 365 admin center** by clicking 'Show All' under the menu and selecting **Azure Active Directory** within the **Admin centers** section:
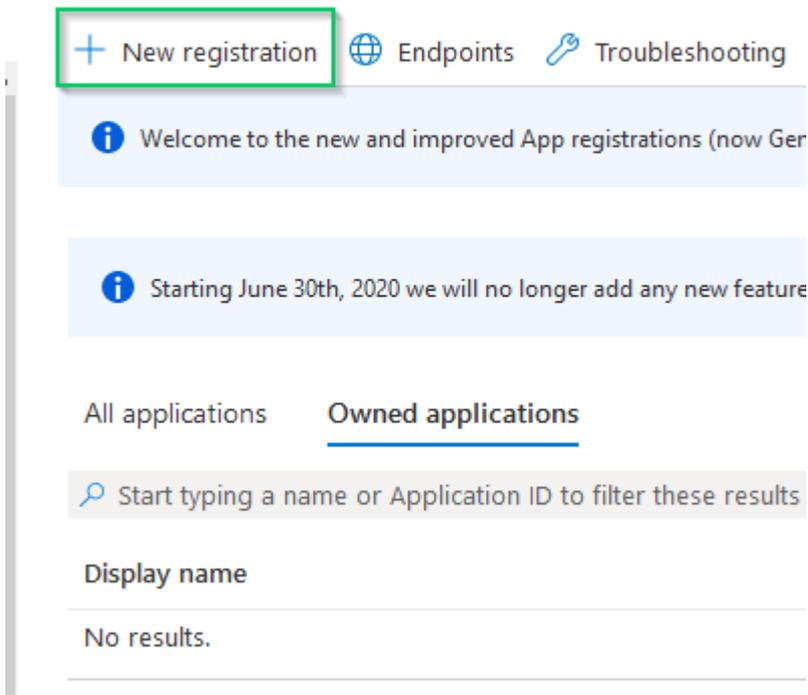


Once in your **Azure Active Directory admin center**, you will need to navigate to **App registrations.** First, make sure you have selected **Azure Active Directory** from the menu, then select **App registrations** from the menu.
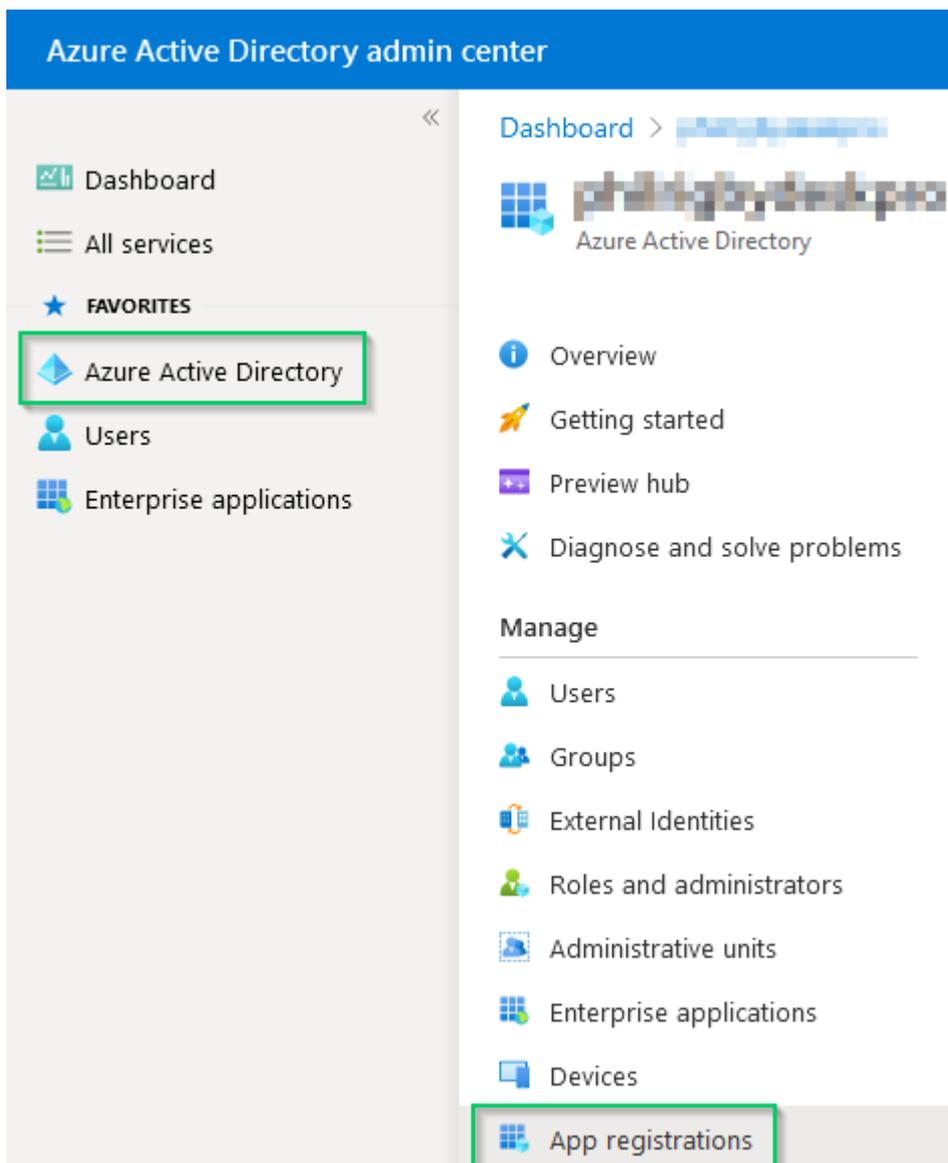
We now need to register a new application for your OAuth2 integration. To do this, first select **New registration** at the top of the page.

To register an application, you need to fill out the following details:

**Name:** This is an identifying name for the app, so you know where it is used.

**Supported account types**: This requires a Multitenant account, i.e. '*Accounts in any organizational directory (Any Azure AD directory – Multitenant)*'

**Redirect URI**: This is where you specify the URI the application will redirect the user after login. For this, you will need to use *https://<helpdesk_url>/admin/office365/token*, replacing the *<helpdesk_url>* with the URL for your helpdesk. (**Note:** This requires https, so you will need to have configured an SSL certificate for your helpdesk before continuing. – This is standard for Deskpro Cloud accounts)

Once you have filled out the form correctly, click the 'Register' button at the bottom of the page

This should now create an app which will be available within the App registrations page.



If you click on the **Display name** for the application, you should see a brief overview of the application. From this list, you will need to make a note of the **Application (client) ID**. You should also confirm that the **Redirect URIs** specifies that there is at least **1 web** redirect in place.

^ Essentials

Display name
Deskpro

Application (client) ID
167071a1-0c9c-43c1-9c45-6dfd400a33ed

Directory (tenant) ID
d0070a32-58f9-456f-933e-cf72e5638957

Object ID
31072df8-2b84-40ca-b643-1fb97b2d7d3f

Supported account types
Multiple organizations

Redirect URIs
1 web, 0 spa, 0 public client

Application ID URI
Add an Application ID URI

Managed application in local directory
Deskpro

We now need to create a client secret in order to connect to the app. Within the App settings, select **Certificates & secrets** from the menu, then select **New client secret** within that page.



Manage

▣ Branding

⊃ Authentication

🔑 Certificates & secrets

▐▌ Token configuration

⊶ API permissions

☁ Expose an API

▦ Owners

🔒 Roles and administrators | Previ...

▢ Manifest

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

| Description | Expires | Value |
| --- | --- | --- |

No client secrets have been created for this application.

This requires an identifying **description** and an **expiry date** set. These can be whatever you want, but we recommend setting the secret to never expire to prevent you from having to create a new secret and login again when the old secret expires. Click the **'Add'** button to create the secret.

This will create a new **Client Secret** associated with this application.

**Please note:** This client secret will not be available if you leave this page or close the window, so we highly recommend making a note of secret by clicking the **Copy** icon at the end of the line. It may also take a few minutes for the  client secret to activate, so if you are experiencing a *invalid_client* error, please wait a few moments and try again.



You should now have the **Client ID** and **Client Secret** required to configure your OAuth2 integration within Deskpro.