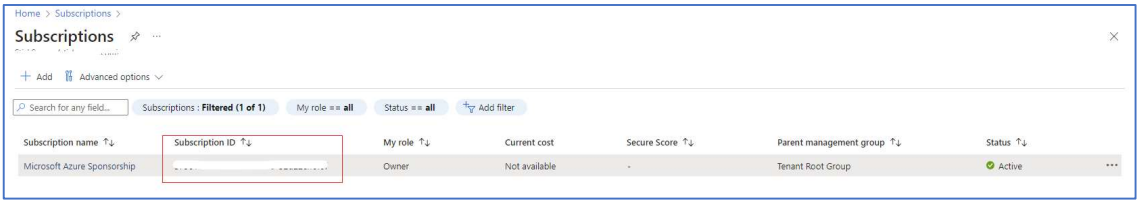
Stick

Your friendly compliance and security platform.

Azure Integration

Azure Integration

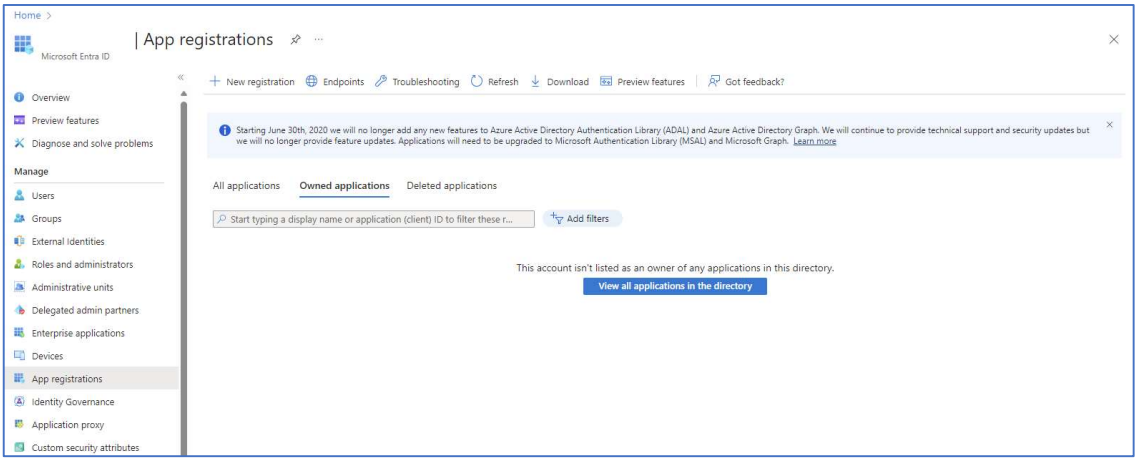
1. Login to the Azure Portal and access the **Subscriptions** panel. Make note of the Subscription ID that includes the resources for scanning.



2. Copy/Paste the **Subscription ID** into notepad. This value is required for Azure scanning.

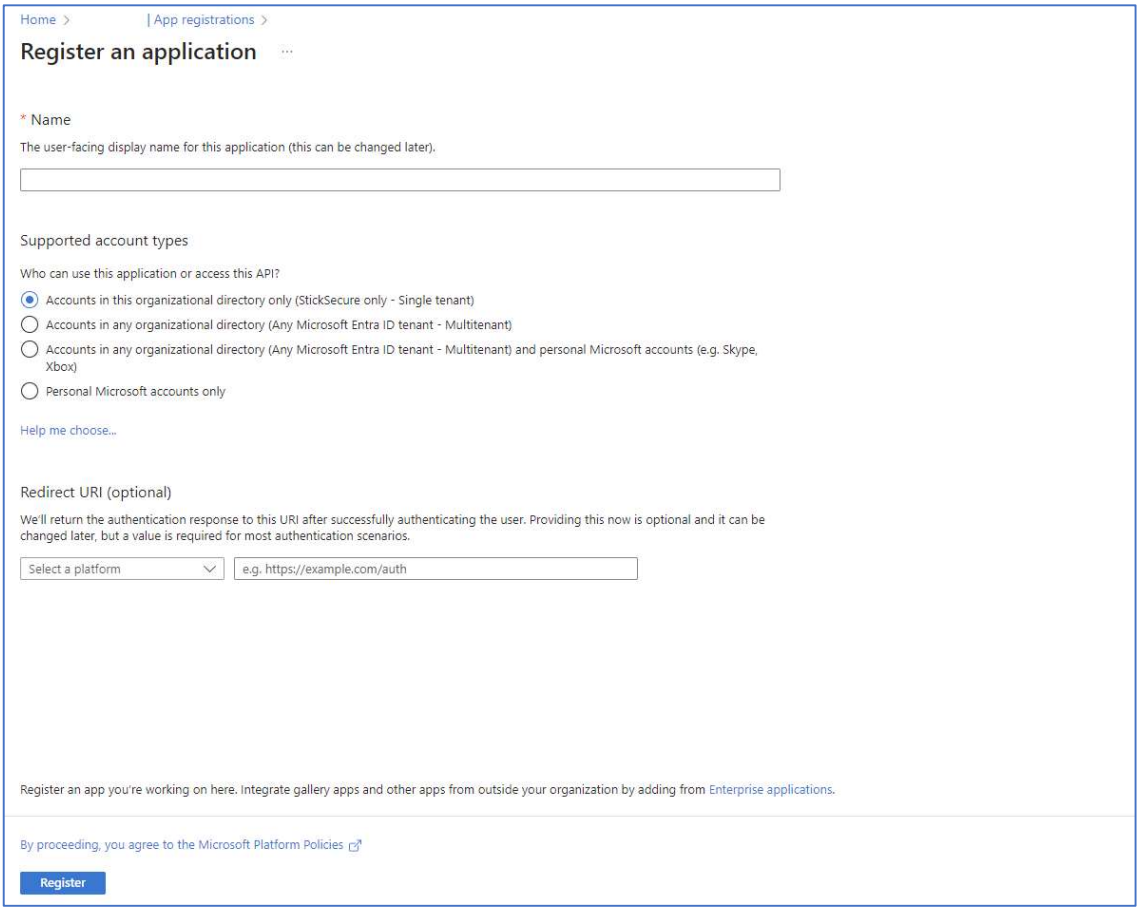
3. Return to the portal home page and click **Microsoft Entra ID.**

4. Click **App Registrations.**



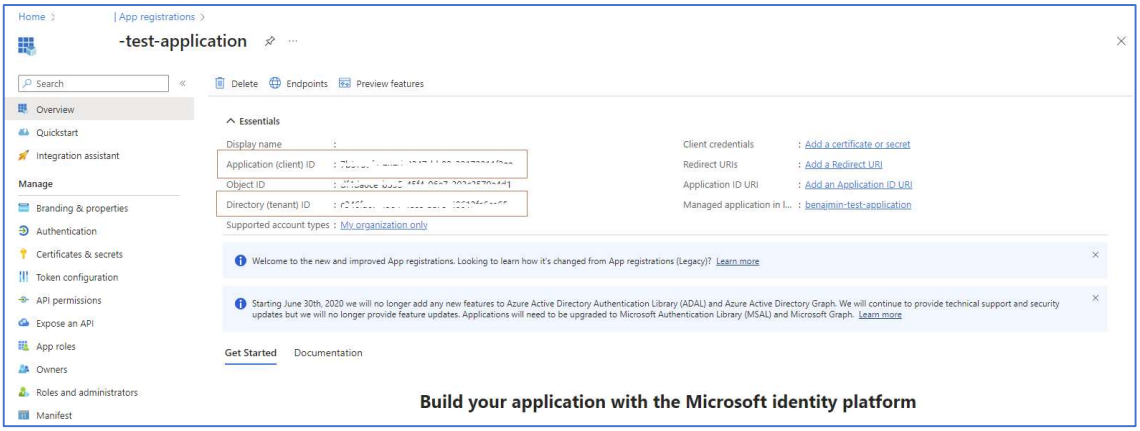
5. Click **New registration**.

6. Enter a name to best identify the App Registration to its purpose. Leave all other settings as their default.



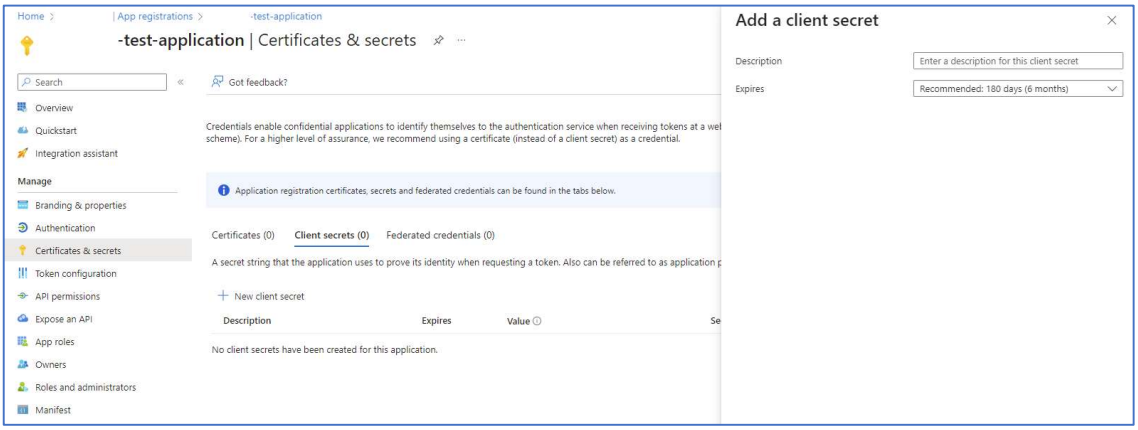
7. Click **Register** to create the App Registration.

8. One the summary page copy/paste the **Application (client) ID** and **Directory (tenant) ID** to notepad.



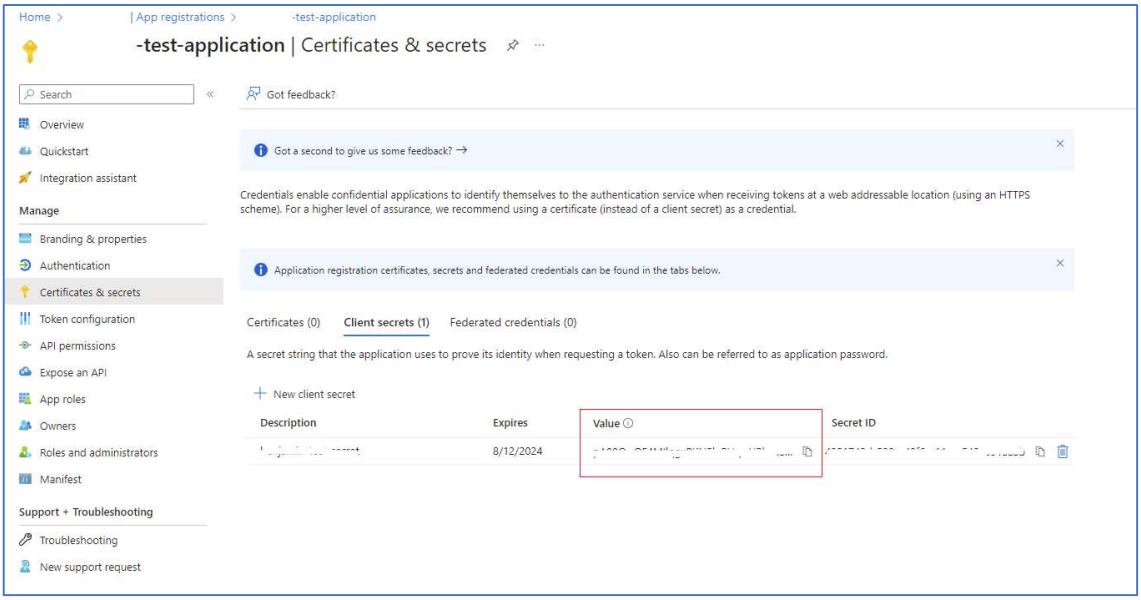
9. Click **Certificates and Secrets**

10. Click **New client secret** and enter a **Description** (e.g. Steampipe Scanner)



11. Click **Add** to create the new Client secret.

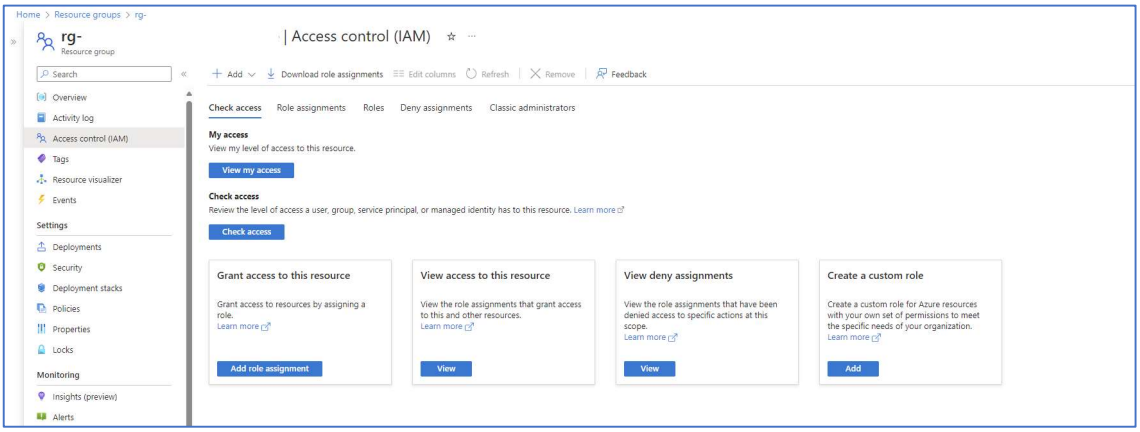
12. Copy/Paste the **Value** from the created Client secret into notepad. **Note**: You will not be able to retrieve this value after navigating away from the page.



The created App Registration should now be granted access to the resources intended for scanning by Steampipe. The below are details on attaching at the resource group level. This allows the Steampipe query engine read access to all resources container within the selected resource group.

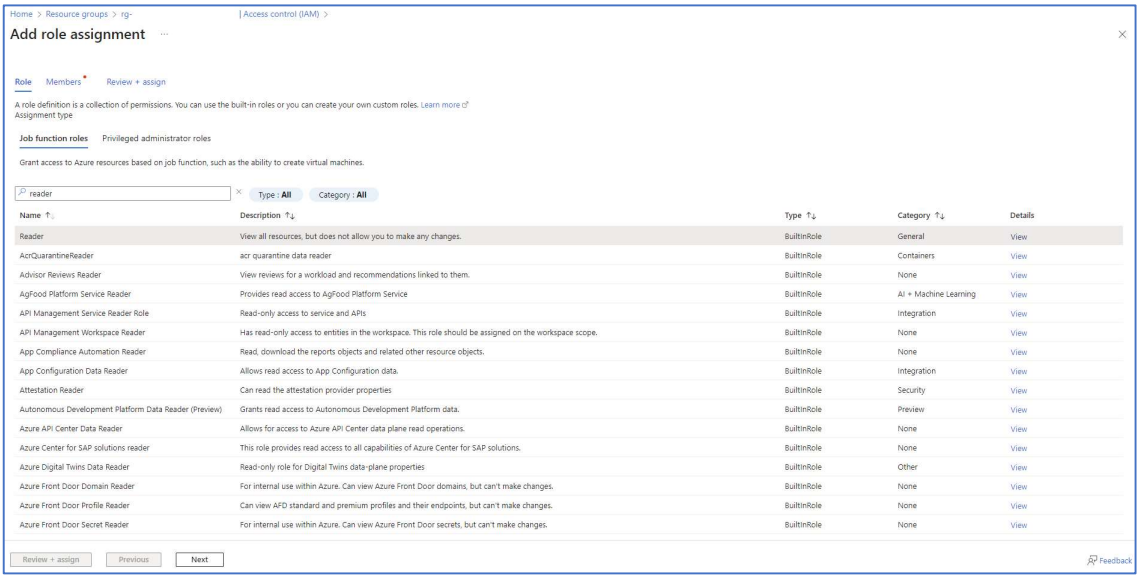
1. In the Azure Portal select a Resource Group to assign the App Registration profile to.

2. Click **the Access control (IAM)** link in the left panel.



3. Click Add -> Add Role Assignment

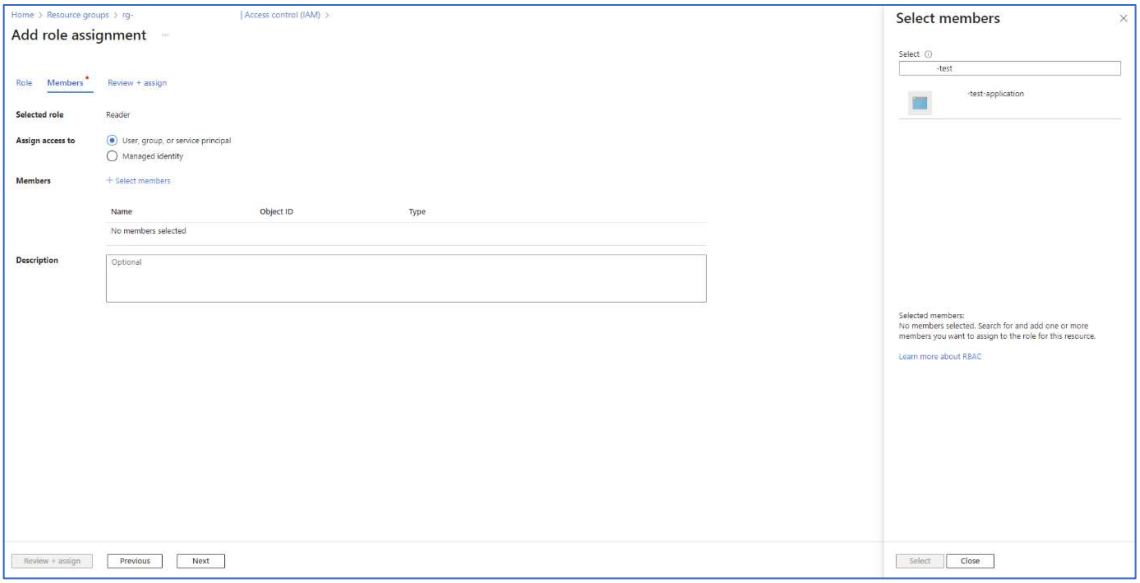
4. Enter **Reader** in the search panel and select **Reader** from the available Job function roles.



5. Click **Next**

6. On the Members tab set Assign access value to User, group, or service principal and click Select members.

7. In the Select members panel search for the name of the application created above and add them to the members.



8. Click **Select**

9. Click **Review + assign**

10. This process has now set up the created Application Registration to have read permissions to the selected resource.

The copy/pasted details from above are to be used when registering a new Azure or MS 365 profile in Stick Secure. Those values are:

Subscription ID, Tenant ID, Client ID, Client Secret