As part of Altocapa signup, permission need to be granted for cloud monitoring. These permissions can be setup at any time during or after signup and the following instructions are also made available during signup.

Azure monitoring permission setup

In order for Altocapa to retrieve the information and metrics necessary to make cost saving recomendations, the following limited permission needs to be granted to the Altocapa application in the Azure subscription/s that will be monitored.

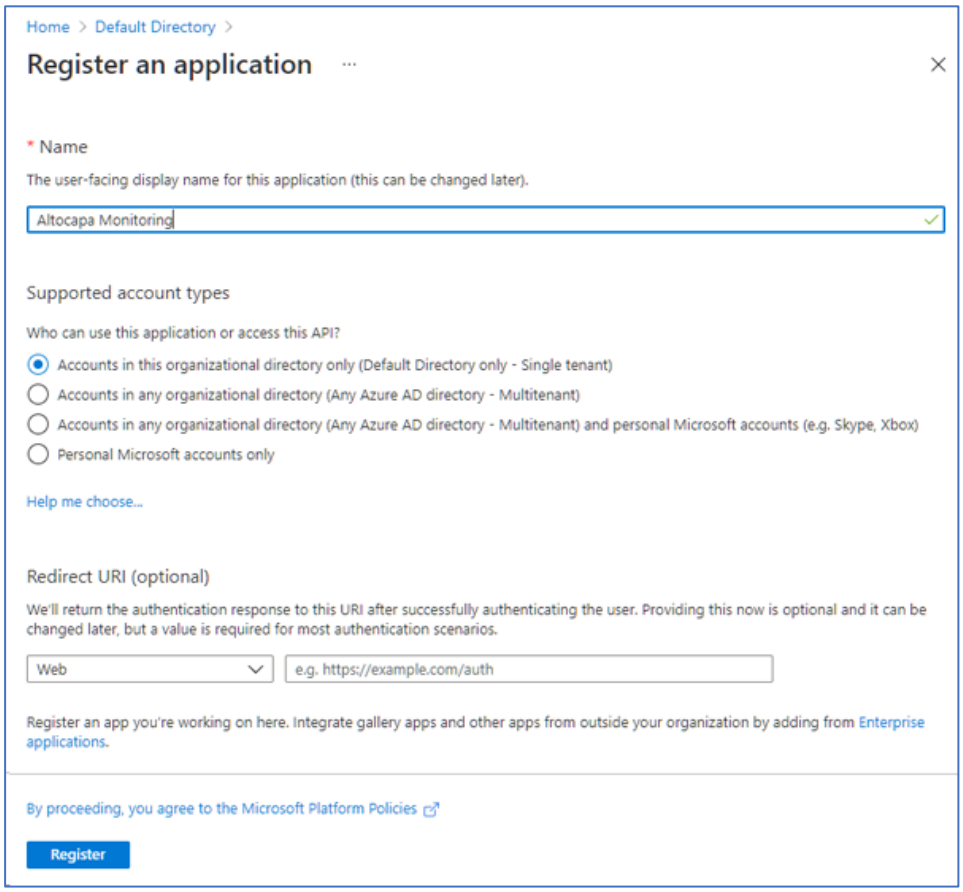
On initial sign-up Altocapa allows for the details of just one Azure Tenant to be added.

The Monitoring Reader and Billing Reader role will need to be assigned by someone with Active Directory Application Administrator rights in your organisation. Global Administrators will have these rights by default.

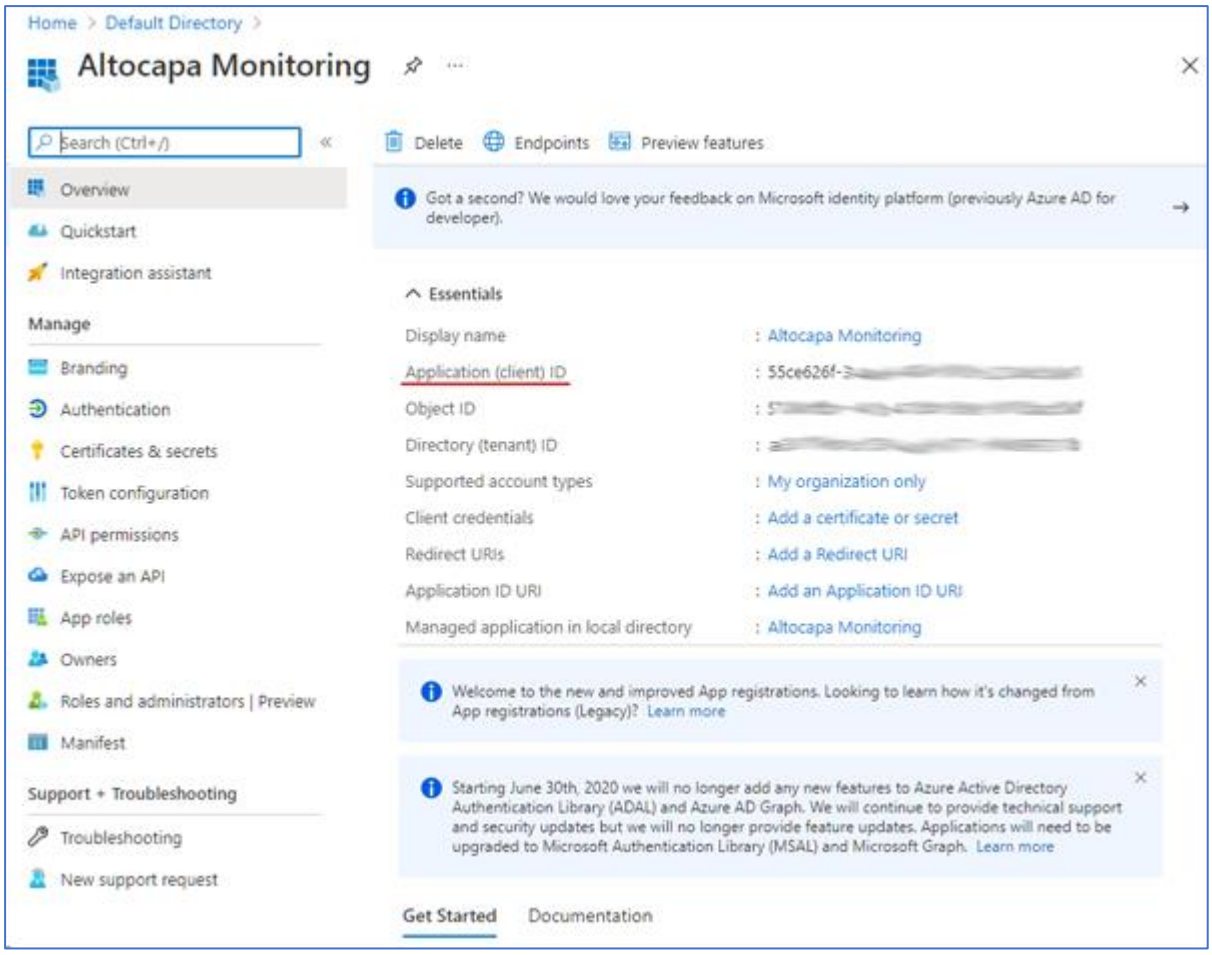
Step by Step Instructions

1. Register the Altocapa Application in Azure Active Directory

- Log in to the Azure portal and open 'Azure Active Directory > App Registrations > New Registration' and fill in the details as per screen shot



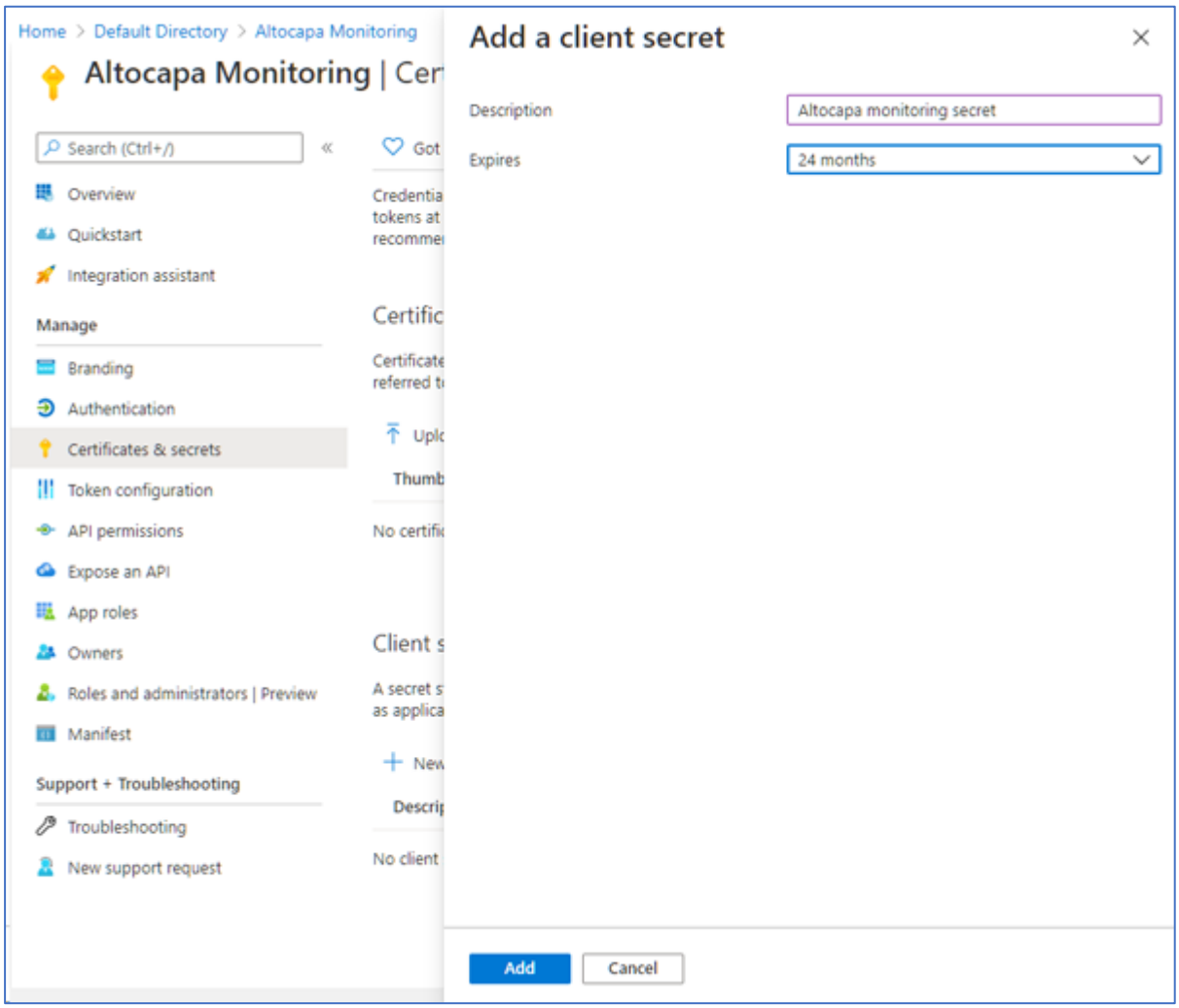
- Click 'Register'



- Make a note of the Application (Client) ID of the newly created registration
- Also make a note of the Directory (tenant) ID

2. Generate a client secret

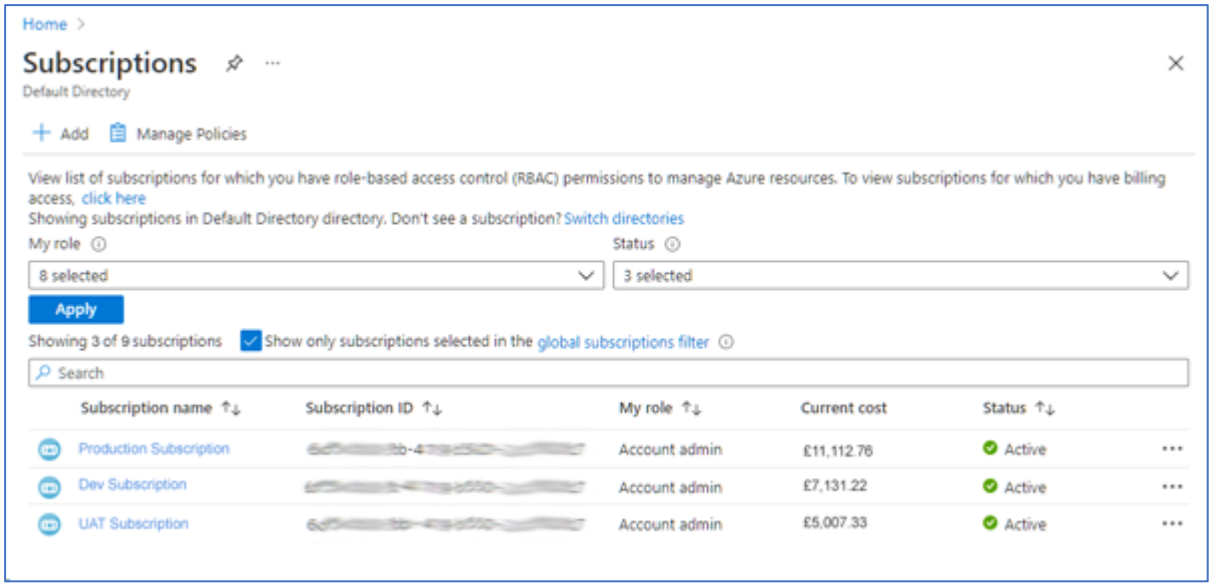
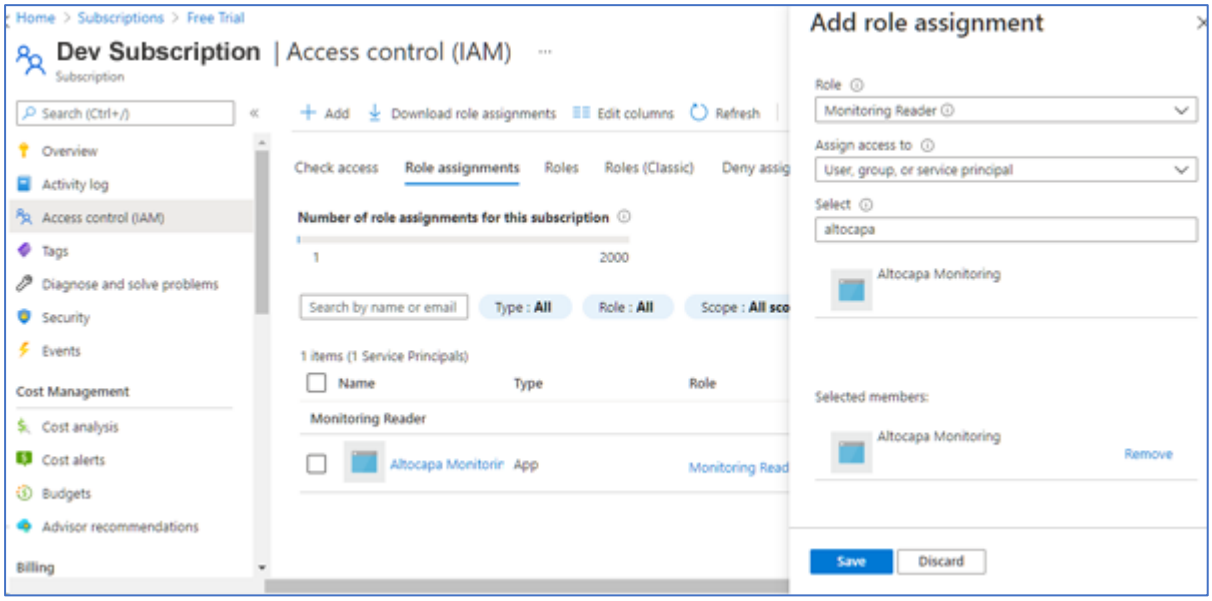
- Click 'Add a certificate or secret' and then click '+ New client secret'



- Fill in details and click 'Add'
- Make a note of the newly created secret value
- This secret together with the client id in the previous step will be required to grant access to Altocapa to access your system.

3. Add this application to the Monitoring Reader & Billing Reader role for the subscription(s) that should be monitored.

- Open the Subscription page as below and click each subscription to Grant access to each subscription to be monitored as per following steps



- Click 'Access control (IAM) > Role Assignments' and click 'Add'
- Allocate the newly created Azure AD application to the built-in Monitoring Reader role and Billing Reader roles.