

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 recommendations, 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

Home > Default Directory >

Register an application

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

Altocapa Monitoring ✓

Supported account types
Who can use this application or access this API?

- Accounts in this organizational directory only (Default Directory 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.

Web e.g. https://example.com/auth

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

- Click 'Register'

The screenshot displays the Azure portal interface for an application registration named 'Altocapa Monitoring'. The left-hand navigation pane includes sections for 'Overview', 'Quickstart', 'Integration assistant', 'Manage' (with sub-items like Branding, Authentication, Certificates & secrets, etc.), and 'Support + Troubleshooting'. The main content area shows the 'Essentials' section with the following details:

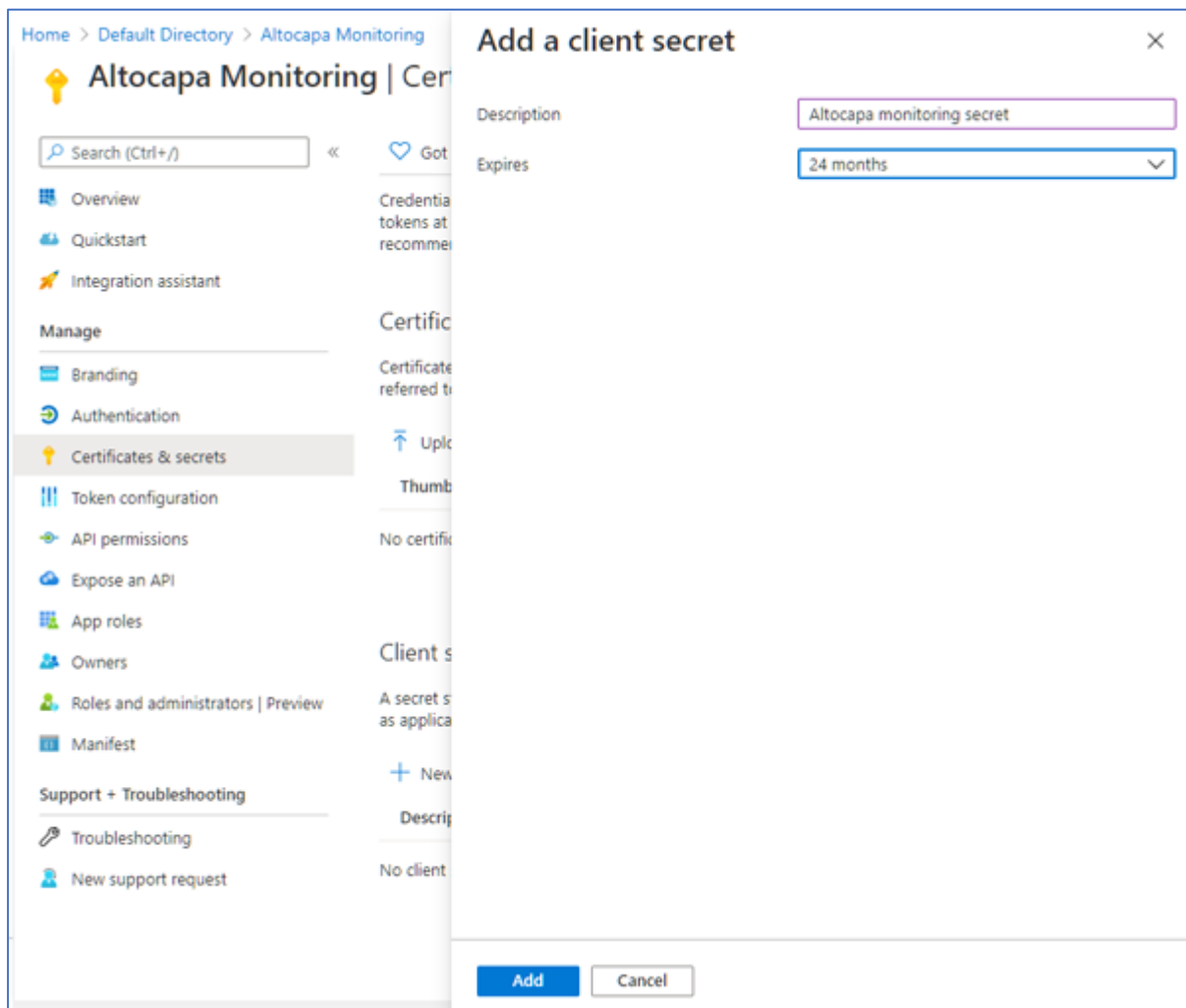
Display name	: Altocapa Monitoring
<u>Application (client) ID</u>	: 55ce626f- [redacted]
Object ID	: [redacted]
Directory (tenant) ID	: [redacted]
Supported account types	: My organization only
Client credentials	: Add a certificate or secret
Redirect URIs	: Add a Redirect URI
Application ID URI	: Add an Application ID URI
Managed application in local directory	: Altocapa Monitoring

Below the essentials, there are two informational messages: one welcoming users to the new and improved App registrations and another regarding the deprecation of Azure Active Directory Authentication Library (ADAL) and Azure AD Graph starting June 30th, 2020. At the bottom, there are links for 'Get Started' and 'Documentation'.

- 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'

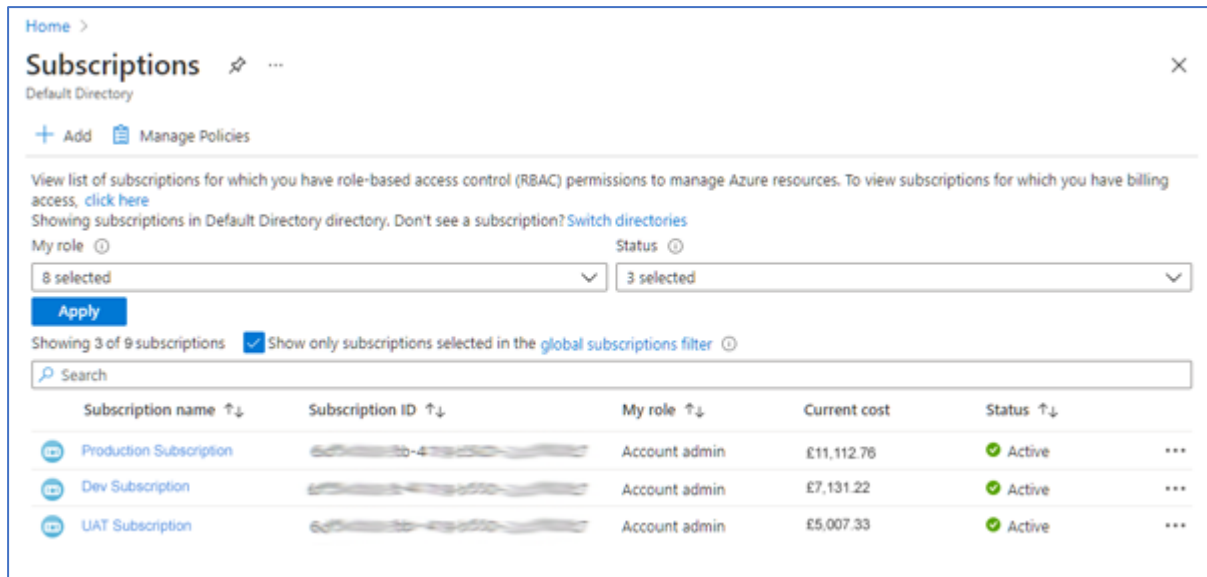


The screenshot shows the 'Add a client secret' dialog box in the Azure portal. The dialog is titled 'Add a client secret' and has a close button (X) in the top right corner. It contains two input fields: 'Description' with the value 'Altocapa monitoring secret' and 'Expires' with a dropdown menu set to '24 months'. At the bottom of the dialog, there are two buttons: 'Add' and 'Cancel'. The background shows the Azure portal navigation pane with 'Certificates & secrets' selected under the 'Manage' section.

- 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.

