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.

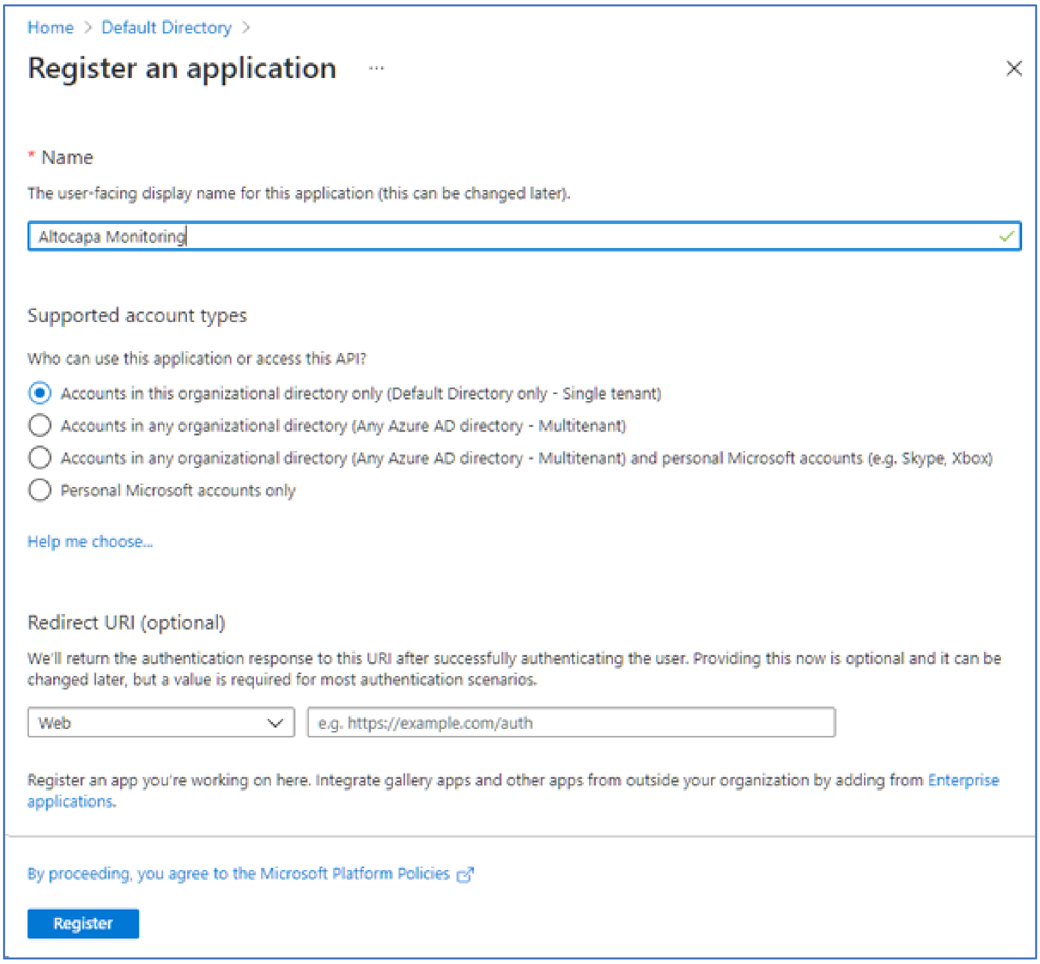
On initial sign-up Altocapa allows for the details of just one Azure Tenant to be added.

The Monitoring Reader 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

- 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)

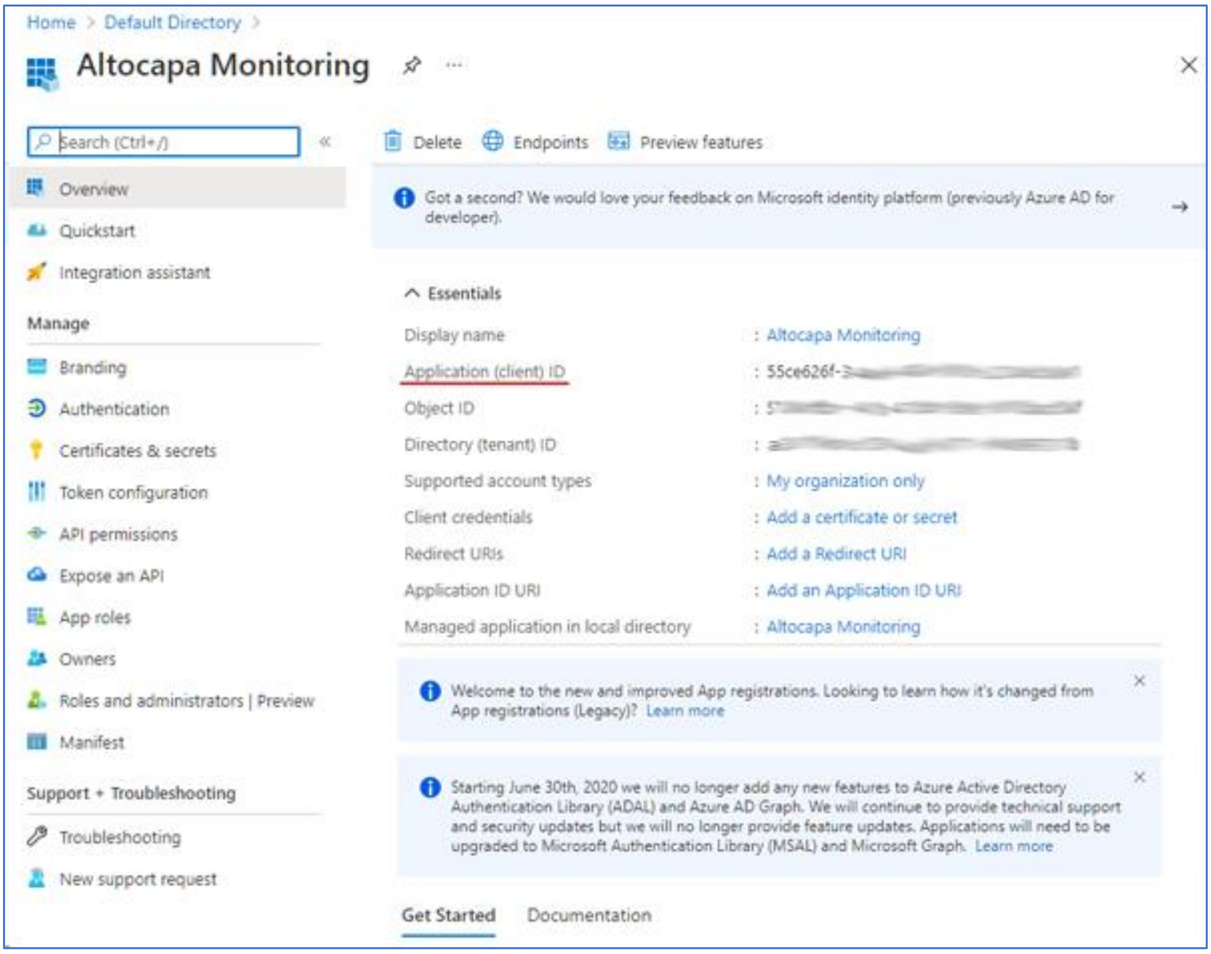
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

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

- Click 'Register'



Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer).

Essentials

Display name	: Altocapa Monitoring
Application (client) ID	: 55ce626f-3[redacted]
Object ID	: 5[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

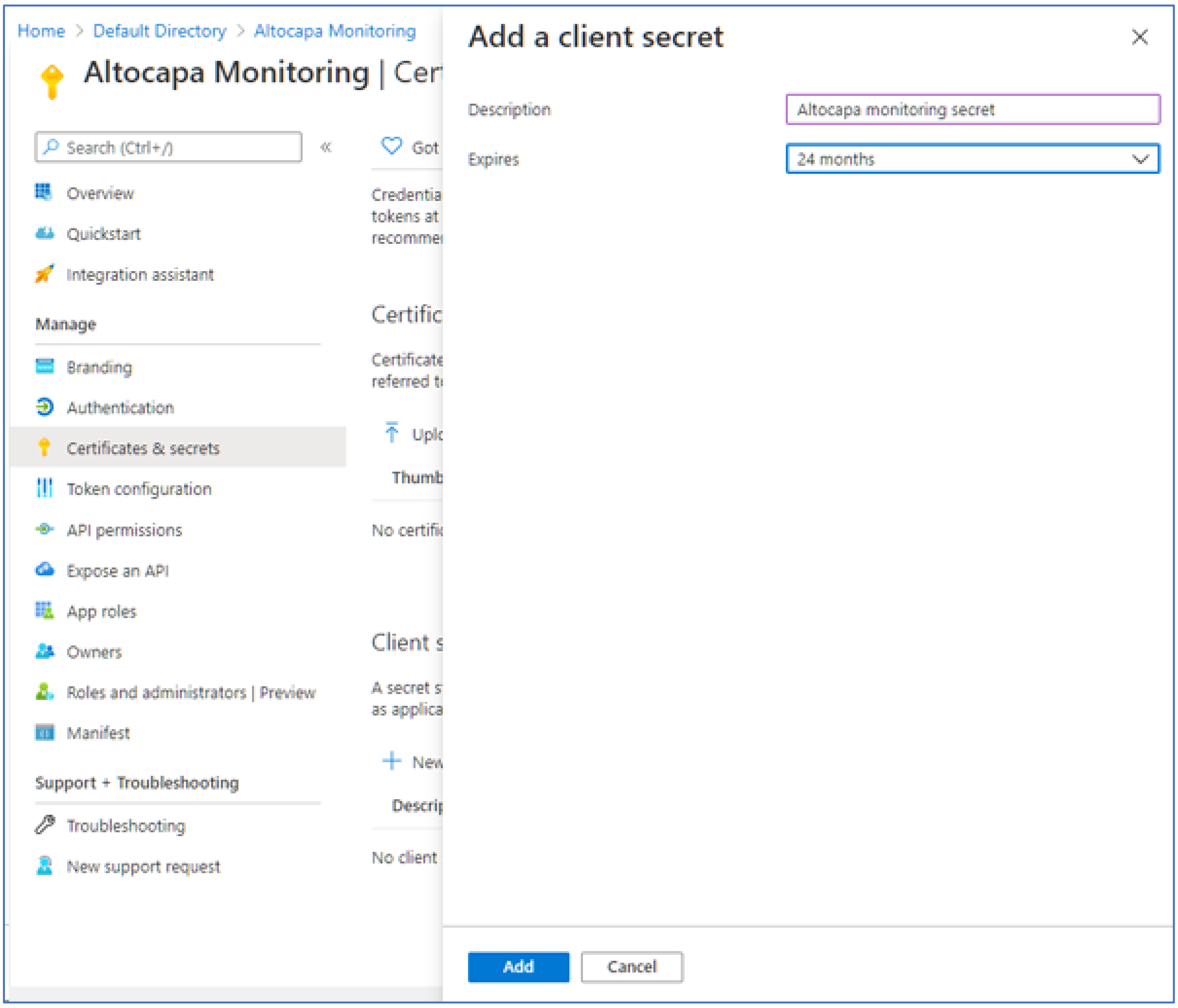
Welcome to the new and improved App registrations. Looking to learn how it's changed from App registrations (Legacy)? Learn more

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. Learn more

- 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'



Add a client secret

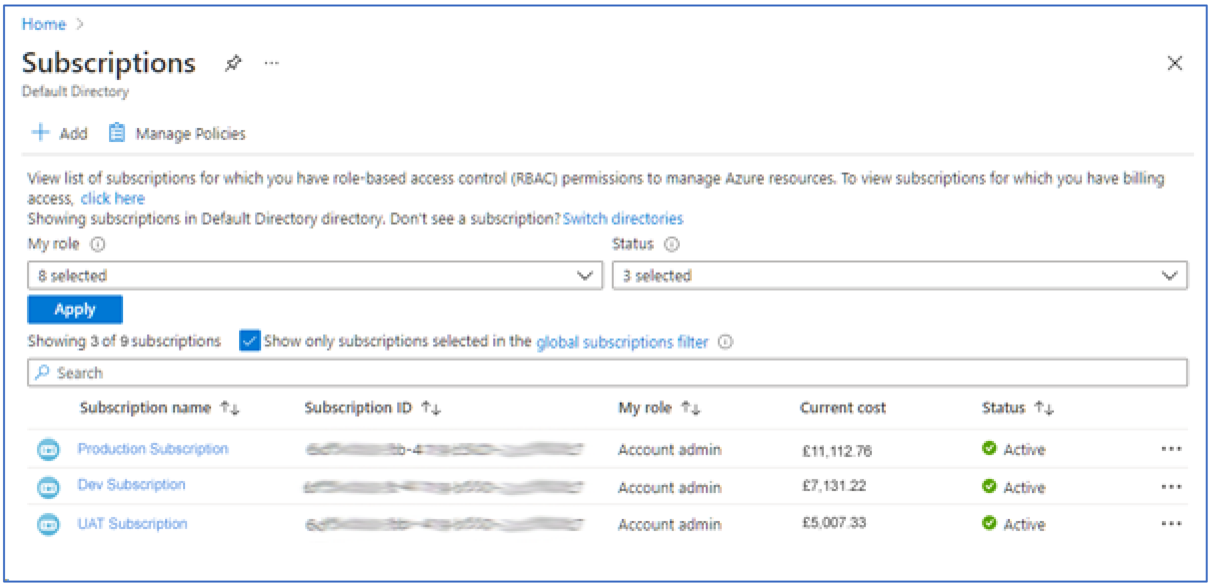
Description: Altocapa monitoring secret

Expires: 24 months

- 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 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



View list of subscriptions for which you have role-based access control (RBAC) permissions to manage Azure resources. To view subscriptions for which you have billing access, click here

Showing subscriptions in Default Directory directory. Don't see a subscription? Switch directories

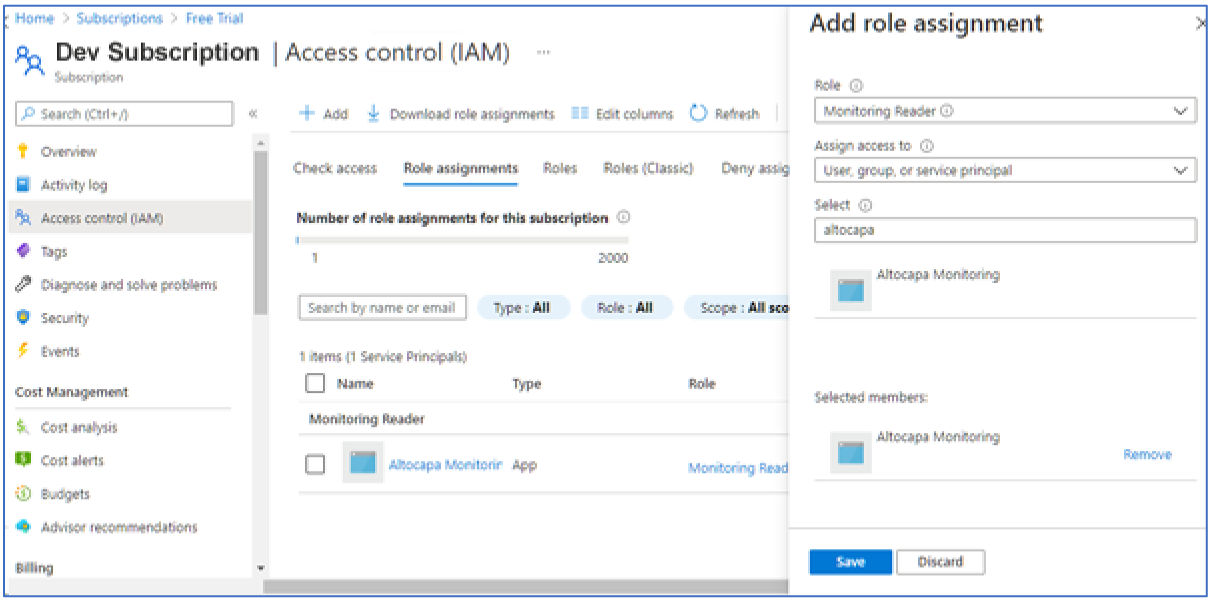
My role: 8 selected

Status: 3 selected

Showing 3 of 9 subscriptions ☑ Show only subscriptions selected in the global subscriptions filter

Subscription name	Subscription ID	My role	Current cost	Status
Production Subscription	[redacted]	Account admin	£11,112.76	Active
Dev Subscription	[redacted]	Account admin	£7,131.22	Active
UAT Subscription	[redacted]	Account admin	£5,007.33	Active

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



Number of role assignments for this subscription: 1 / 2000

1 items (1 Service Principals)

Name	Type	Role
Monitoring Reader		
Altocapa Monitorir	App	Monitoring Read

Add role assignment

Role: Monitoring Reader

Assign access to: User, group, or service principal

Select: altocapa

Altocapa Monitoring

Selected members:

Altocapa Monitoring