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 <u>Monitoring Reader</u> and <u>Billing Reader</u> 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?
<ul> <li>Accounts in this organizational directory only (Default Directory only - Single tenant)</li> </ul>
Accounts in any organizational directory (Any Azure AD directory - Multitenant)
O 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  v 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'

Home > Default Directory > Altocapa Monitoring	g 🖈 …		×
P §earch (Ctrl+/) ≪	📋 Delete 🜐 Endpoints 🔚 Preview fea	atures	
Uverview Overview	Got a second? We would love your feedbac	k on Microsoft identity platform (previously Azure AD for	<i>→</i>
😃 Quickstart	developer).		
💉 Integration assistant	∧ Essentials		
Manage	Display name	: Altocapa Monitoring	
Branding	Application (client) ID	: 55ce626f-3	
Authentication	Object ID	:5	
📍 Certificates & secrets	Directory (tenant) ID	1.8	
III Token configuration	Supported account types	1 My organization only	
API permissions	Client credentials	: Add a certificate or secret	
C Expose an API	Redirect URIs	: Add a Redirect URI	
App roles	Application ID URI	: Add an Application ID URI	
	Managed application in local directory	: Altocapa Monitoring	
Owners     Roles and administrators   Preview     Manifest	Welcome to the new and improved App App registrations (Legacy)? Learn more	o registrations. Looking to learn how it's changed from	×
Support + Troubleshooting	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		
New support request	Get Started 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'

Home > Default Directory > Altocapa Mo		Add a client secret		×
	green	Description	Altocapa monitoring secret	
✓ Search (Ctrl+/) «	💙 Got	Expires	24 months	~
Overview	Credentia tokens at			
😃 Quickstart	recomme			
💉 Integration assistant				
Manage	Certific			
Branding	Certificate referred to			
Authentication	-			
📍 Certificates & secrets	T Upk			
Token configuration	Thumb			
<ul> <li>API permissions</li> </ul>	No certific			
Expose an API				
App roles				
A Owners	Client s			
8 Roles and administrators   Preview	A secret s as applica			
III Manifest				
Support + Troubleshooting	+ New			
Troubleshooting	Descrip			
Rew support request	No client			
		Add Cancel		

- 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

	Directory					×
access	list of subscriptions for which y s, click here ing subscriptions in Default Di	vou have role-based access control (RBAC) pern rectory directory. Don't see a subscription? Swit	-	e resources. To view subsc	riptions for which you ha	ve billing
8 se	lected	~	3 selected			~
Show	pply ing 3 of 9 subscriptions 🗸 S earch	how only subscriptions selected in the global s	ubscriptions filter 🛈			
	Subscription name $\uparrow_\downarrow$	Subscription ID $\uparrow_{\downarrow}$	My role ↑↓	Current cost	Status ↑↓	
	Production Subscription	60 3-47 550 5	Account admin	£11,112.76	<ul> <li>Active</li> </ul>	
	Dev Subscription	6700-07	Account admin	£7,131.22	<ul> <li>Active</li> </ul>	
œ	UAT Subscription		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 and Billing Reader roles.

Home > Subscriptions > Free Trial		Add role assignment	
	Access control (IAM)	5	
Subscription		Role 🕕	
P Search (Ctrl+/) «	🕂 Add 🛓 Download role assignments 🔳 Edit columns 🖒 Refresh	Monitoring Reader ③	~
Overview		Assign access to ①	
Activity log	Check access Role assignments Roles Roles (Classic) Deny	User, group, or service principal	~
Access control (IAM)	Number of role assignments for this subscription 💿	Select ③	
	Number of role assignments for this subscription (	altocapa	
Tags	1 2000	Altocapa Monitoring	
Diagnose and solve problems	Search by name or email Type : All Role : All Scope : Al		
Security	search by name or email Type : All Role : All Scope : Al	I SCO	
🗲 Events	1 items (1 Service Principals)		
Cost Management	Name Type Role	Selected members:	
\$. Cost analysis	Monitoring Reader		
Cost alerts	Attocapa Monitorin App Monitoring		Remove
③ Budgets			
Advisor recommendations			
Billing •		Save Discard	