# Microsoft Office 365 API Provider Setup

Last Modified on 12/30/2019 8:49 pm EST

### **Overview**

In order to authenticate an instance of the Microsoft Dynamics 365 connector, you must have the following:

- A Microsoft Azure Active Directory account
- A Microsoft Office 365 account
- A web application registered and configured with Azure Active Directory

## Registering and Configuring a Web Application with Azure Active Directory

There are several required steps to registering and configuring a new web application in Azure AD. This section covers these steps, which include:

- Registering your application in the Azure Portal
- Recording the application ID
- Generating and recording the client secret
- Setting App permissions

## Registering your Application in the Azure Portal

- 1. In a web browser, navigate to the Azure Portal and sign in using your Azure Active Directory credentials.
- 2. From the left-hand navigation toolbar, select **Azure Active Directory** and then select **App registrations**.



#### 3. Select New registration.

Microsoft Azure	♀ Search re	sources, services, and docs		>_	P	Q	ŝ	?	$\odot$	cloudeleme CL
	«	Home > cloud elements - App registr	ation	s						
+ Create a resource		cloud elements - App regis	trati	ions			_			
A Home			«	+ 1	lew regis	tration	🕀 End	dpoints	🗙 Tro	ubleshooting
<ul> <li>Dashboard</li> <li>All services</li> </ul>		(i) Overview	1	0	Welcome new	to the n	iew and in	nproved	App regist	rations (now Gen
— ★ FAVORITES ————		😴 Getting started			5					p registrations
🔇 App Services		Manage			Still war	t to use	App regi	istrations	s (Legacy	? Go back and t
SQL databases		Sers Users		All	applicat	ions _	Owned a	applicat	ions	

4. On the Register an application screen, enter a name for your application in the Name field, and then click Register; the supported account types and redirect URI will be configured later during this process. For more information on the application registration process, see Microsoft's documentation.

## Recording the Application ID

After registering your new application, record the Application (client) ID as displayed in your application's overview page. You will use this string as the API key when you authenticate a connector instance.

Home > cloud elements - App registra	tions > myCoolApp				
myCoolApp					
«	🛅 Delete 🌐 Endpoints				
Reverview	Display name				
🗳 Quickstart	myCoolApp				
Manage	Application (client) ID				
🚾 Branding	Directory (tenant) ID				
Authentication	Object ID				
📍 Certificates & secrets	CONTRACTOR AND AND ADDRESS OF				

## Generate and Record the Client Secret

1. Click Certificates & secrets.



2. On the Certificates & secrets page, click the New client secret button.

🔶 myCoolInstance - Certifi	cates & secrets		X	? >
	Credentials enable applications to identify	themselves to th	e authentication service when	
Uverview	receiving tokens at a web addressable loca assurance, we recommend using a certifica			of
🗳 Quickstart	Certificates			
Manage	Certificates	*	·	-
s Branding	Also can be referred to as public keys.	the application	s identity when requesting a toke	n.
Authentication	→ Upload certificate			
Certificates & secrets	No certificates have been added for this ap	plication.		
API permissions				
Expose an API	THUMBPRINT STAR	T DATE	EXPIRES	
Owners				
Roles and administrators (Previ	Client secrets			
0 Manifest	A secret string that the application uses to	prove its identit	y when requesting a token. Also c	an
Support + Troubleshooting	be referred to as application password.			
✗ Troubleshooting	+ New client secret			
New support request	DESCRIPTION EXPIRES	VALUE		
	No client secrets have been created for this	application.		

3. In the Add a client secret window, add a name to the Description field, select Never, and then click Add.

Description		
myCoolSec	ret	
Expires		
🔵 In 1 yea	ar	
O In 2 yea		
	415	
Never		

4. Under Client secrets, record the value for your newly created client secret. This value is your client secret, which you will use as the API secret when you authenticate a connector instance.

myCoolInstance - Certifie	cates & secrets			\$	>
	Copy the new client secret	value. You won't be able to	retrieve it after you leave this blade.		
<ul> <li>Overview</li> <li>Quickstart</li> <li>Manage</li> </ul>		g an HTTPS scheme). For	o the authentication service when receiving tokens a a higher level of assurance, we recommend using a		
Branding	Certificates				
<ul> <li>Authentication</li> </ul>	Certificates can be used as sec referred to as public keys.	rets to prove the applicati	on's identity when requesting a token. Also can be		
Certificates & secrets	The Transformation Transformatiis Transformatiis Transformatiis Transformatiis Transformatii				
API permissions	No certificates have been adde	ed for this application.			
Expose an API					
Cwners	THUMBPRINT	START DAT	E EXPIRES		
Roles and administrators (Previ					
0 Manifest	Client secrets				
Support + Troubleshooting	5 11	tion uses to prove its ider	ntity when requesting a token. Also can be referred t	to as	
★ Troubleshooting	application password.				
New support request	+ New client secret				
	DESCRIPTION	EXPIRES	VALUE		
	myCoolSecret	12/31/2299	second entropy of states	Ô	

## Setting App Permissions

After exposing your APIs, you need to set app permissions depending on your requirements.

On the navigation panel to your left, click **API permissions** and then **Add a permission**, as shown in the picture below.

Create a resource	OloudElementsV2 - API p	permissions			,
Home	, Search (Ctrl+/) «	API permissions			
All services FAVORITES	<ul><li>Overview</li><li>Quickstart</li></ul>	opportunity to grant/deny access.	questing permissions.	These permissions show up during the consen	It process where users are given the
Resource groups All resources Recent	Manage Branding	+ Add a permission API / PERMISSIONS NAME	ТҮРЕ	DESCRIPTION	ADMIN CONSENT REQUIRED
App Services	Certificates & secrets     API permissions	Application.ReadWrite.All		Read and write all applications Read and write devices	Yes 🤡 Granted for Default
Virtual machines	<ul> <li>Expose an API</li> <li>Owners</li> </ul>	Directory.ReadWrite.All	Delegated	Read and write directory data Read and write directory data	Yes 🤡 Granted for Default
Cloud services (classic)	<ul> <li>Roles and administrators (Previ</li> <li>Manifest</li> </ul>	Domain.ReadWrite.All Group.ReadWrite.All		Read and write domains Read and write all groups	Yes 📀 Granted for Default
Subscriptions Azure Active Directory Monitor	Support + Troubleshooting	Member.Read.Hidden	5	Read all hidden memberships Read all users' basic profiles	Yes S Granted for Default
Cost Management + Bill	New support request	▼ Microsoft Graph (20)	5	Have full access to user calendars	- 🔗 Granted for Default