Configuring AAD app registration for O365 Management API

Author: Scott Murray – [Scott.Murray@Microsoft.com](mailto:Scott.Murray@Microsoft.com)

Date: 5/1/2019

Summary: This document outlines a specific tested scenario that shows how to configure the O365 Management API app registration leveraging the new API registration process through the AAD portal.

<#

LEGAL DISCLAIMER

This Sample Code is provided for the purpose of illustration only and is not

intended to be used in a production environment. THIS SAMPLE CODE AND ANY

RELATED INFORMATION ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER

EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF

MERCHANTABILITY AND/OR FITNESS FOR A PARTICULAR PURPOSE. We grant You a

nonexclusive, royalty-free right to use and modify the Sample Code and to

reproduce and distribute the object code form of the Sample Code, provided

that You agree: (i) to not use Our name, logo, or trademarks to market Your

software product in which the Sample Code is embedded; (ii) to include a valid

copyright notice on Your software product in which the Sample Code is embedded;

and (iii) to indemnify, hold harmless, and defend Us and Our suppliers from and

against any claims or lawsuits, including attorneys’ fees, that arise or result

from the use or distribution of the Sample Code.

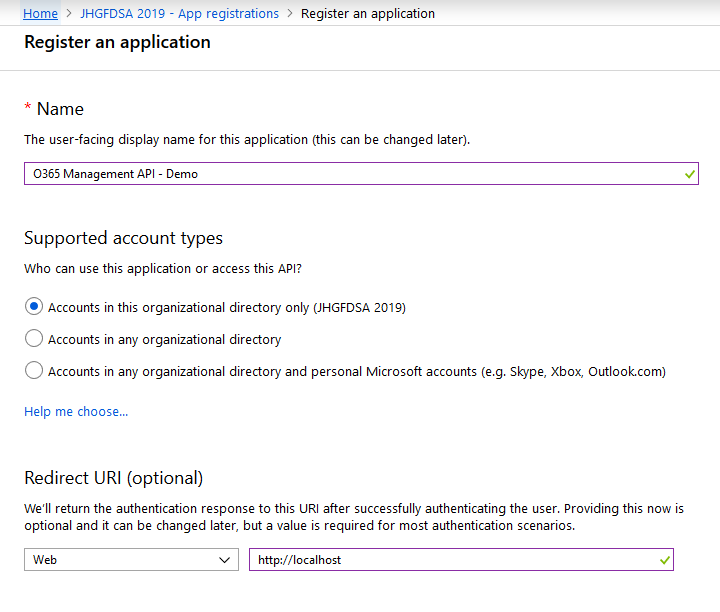
This posting is provided "AS IS" with no warranties, and confers no rights. Use

of included script samples are subject to the terms specified

at http://www.microsoft.com/info/cpyright.htm.

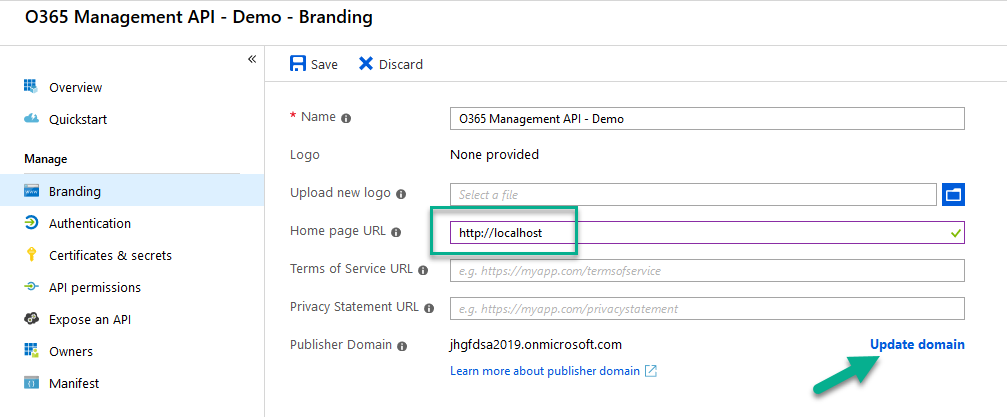
**#>**

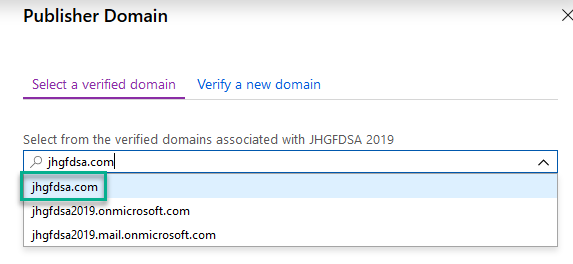
1. Log into portal.azure.com and navigate to Azure Active Directory. Once there, go to App Registrations and hit New registration



Fill out as above and hit Register

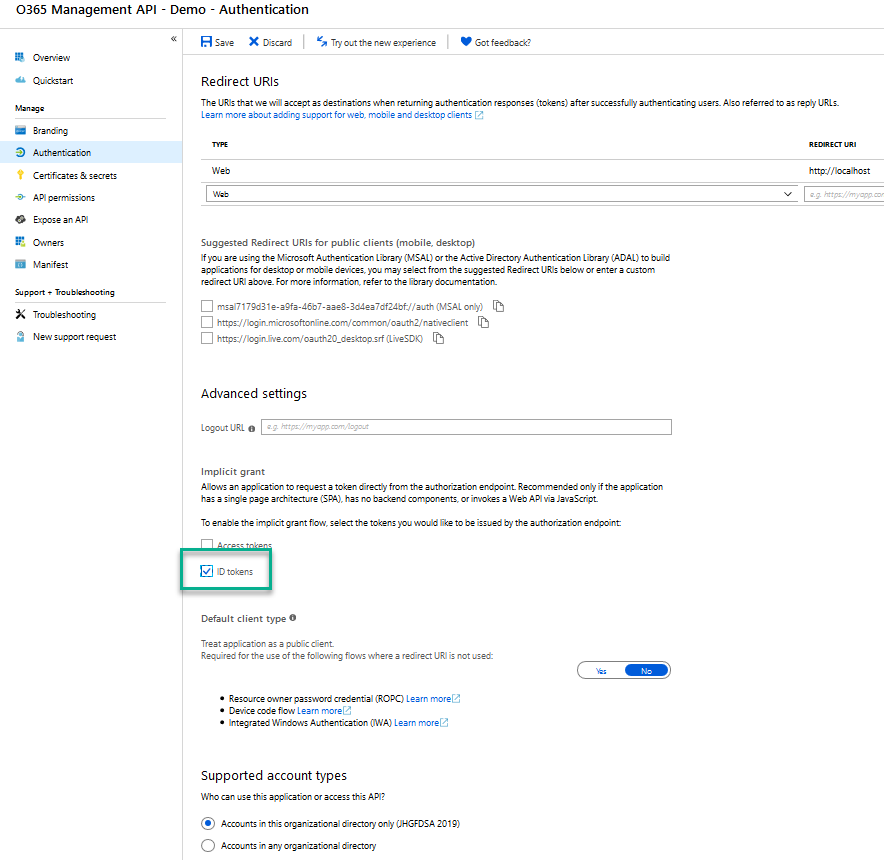
1. Once the registration completes, it is time to configure. Head to branding first and ensure the page is filled out as below





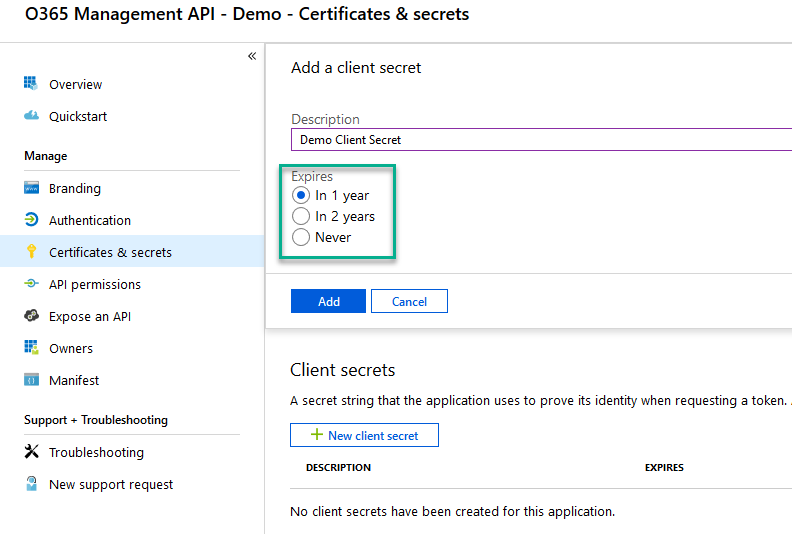
Hit Save at the bottom and then Save at the top

1. Got to Authentication and fill out as follows:



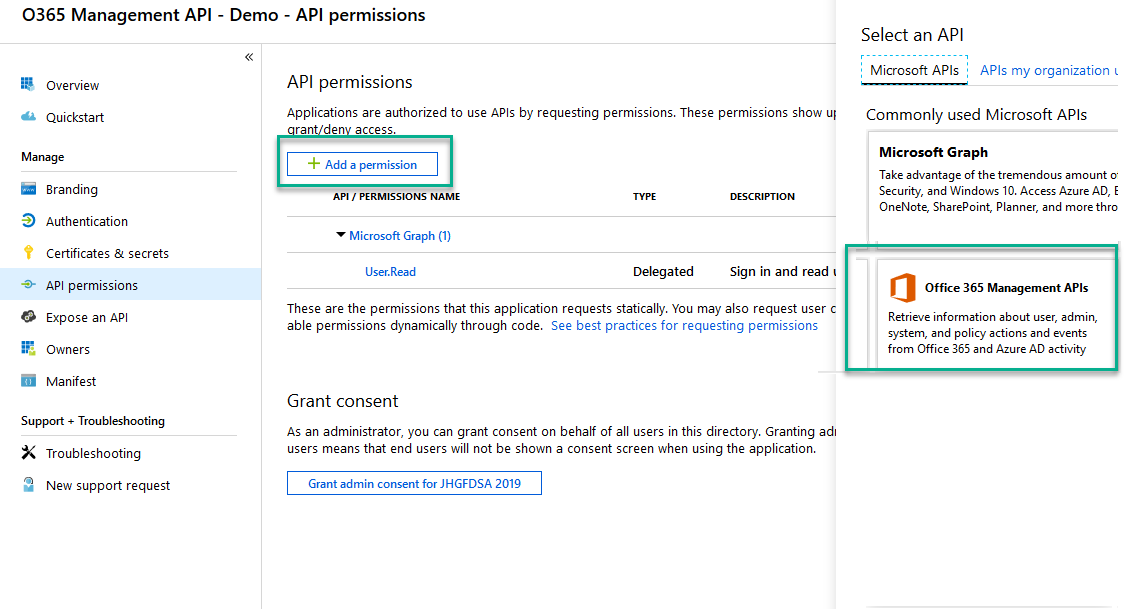
Hit Save at the top

1. Navigate to Certificates & secrets -> New client secret



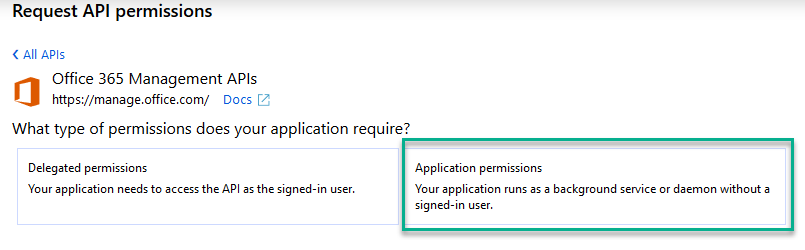
Select a time window that makes sense to you and for your security requirements. Make sure the name you give is informative and will make it easy to keep track of the key. Immediately copy the secret off to a safe location once you save. You will need it for your application connections, and it is only exposed through the UI at this time. You will not be able to retrieve this key again in the future and will have to create a new one.

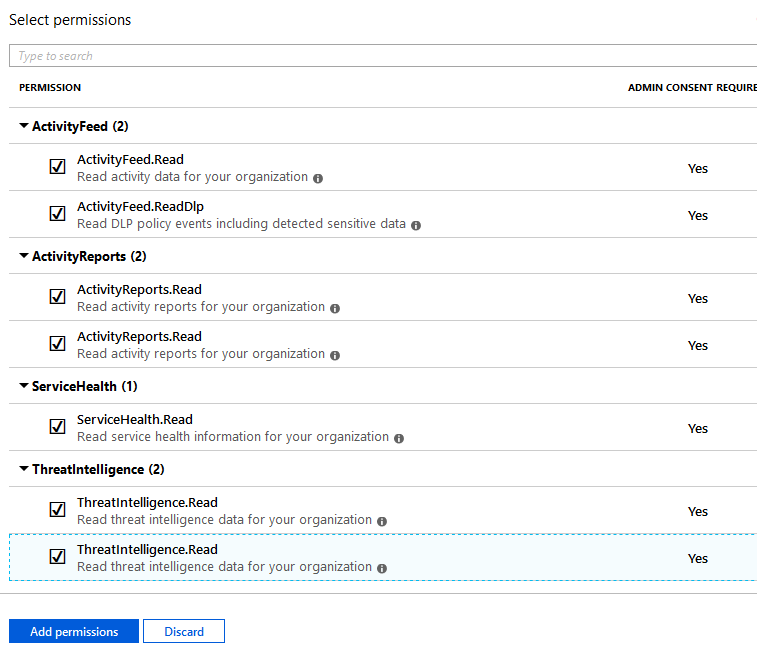
1. Navigate to API Permissions



Add a perm and Select Office 365 Management APIs. Leave the Microsoft Graph permission in place.

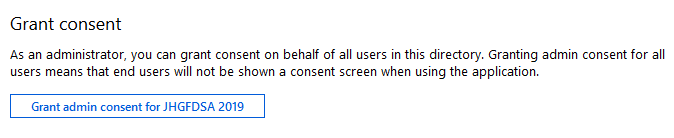
1. Select Application permissions. You do not need to use Delegated permissions for the purposes of retrieving the logging through the Management API





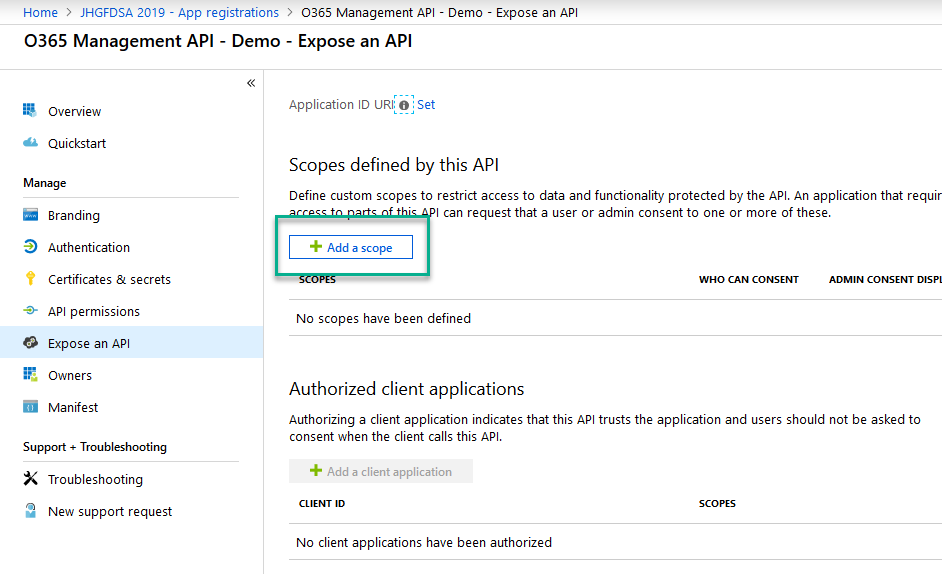
Some of these are deprecated but it is impossible to tell which ones are deprecated through the UI. Select them all and then hit Add permissions.

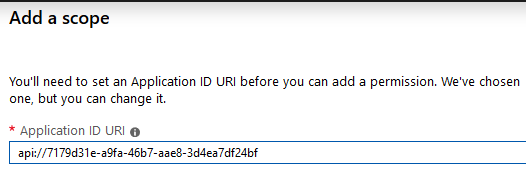
1. Grant admin consent



Hit yes

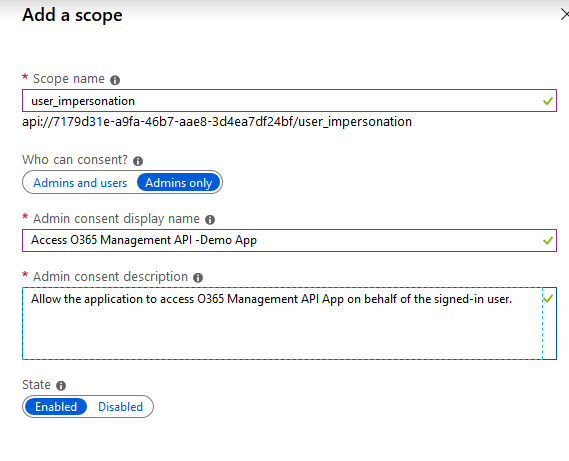
1. Add a scope





You can leave the default for our purposes. Save and continue (be patient).

1. Once it saves, you can further configure. Give the scope a name and fill out as follows



Hit Add scope and you are done.

Return to the Overview tab for the application. With the client secret you have already copied off, also copy the Application (client) ID and the Directory (tenant) ID. These 3 pieces of information are what you need in order to access the O365 Management API through the registered application.