Setup - Azure Lighthouse for CSP

ONLY for Cloud Service Providers / Managed Service Providers OR if the M365 tenant is unequal the Azure tenant

For MSPs / CSPs we provide a different scenario of the Lighthouse setup.

The setup steps are pretty similar to the general setup (Setup - Azure Lighthouse)

However for cloud service providers the scenario can be a different one where CSPs want to run and operate several OfficeExpert instances within their own tenant. We call this a "Distributed Scenario".

Table of Contents

What pieces will be deployed?

Following resources are part of the deployment

- Key Vault
- Function App (incl. App Service Plan)
- Event Hub
- Storage Account
- App Insights + Log Analytics

Deployment Prerequisites

Please make sure that the following Resource providers are registered in the Subscription you use.

Resource Providers
Microsoft.Insights
Microsoft.ContainerInstance
Microsoft.EventHub
Microsoft.Web
Microsoft.KeyVault
Microsoft.OperationalInsights
Microsoft.ManagedIdentity
Microsoft.Storage

Azure Lighthouse

Perform this within the CSP's Azure tenant!

An **Owner** of the Subscription (Owner via RBAC) has to perform the following steps in order to get the Azure Lighthouse template deployed.
This will connect panagenda with the specified azure resource group of the customers tenant (**Note**: panagenda gets Contributor access for the entire Resource Group) !

```
1) Request the template files from panagenda (support@panagenda.com)
2) Create a Resource Group manually (default:  panagenda-azure-lighthouse)
3) Open Azure CLI as an Owner of the subscription
4) Upload the template files via Azure CLI
5) Switch to PowerShell
6) Execute the following command to make sure that the correct SubId is in context
Set-AzContext -Subscription {ID}

7)
# If a Resource Group is used. Adjust the Location and RG parameters depending to your needs
New-AzSubscriptionDeployment -TemplateFile panagenda-azure-lighthouse-rg.json -TemplateParameterFile panagenda-
azure-lighthouse.parameters.json -rgName panagenda-azure-lighthouse -Location WestEurope
```

Graph API Subscription App Registration

Perform this within the target Customer Tenant!

A second Azure AD App registration in the customer tenants needs to be added (beside of the one which is being created/used by the OfficeExpert appliance).

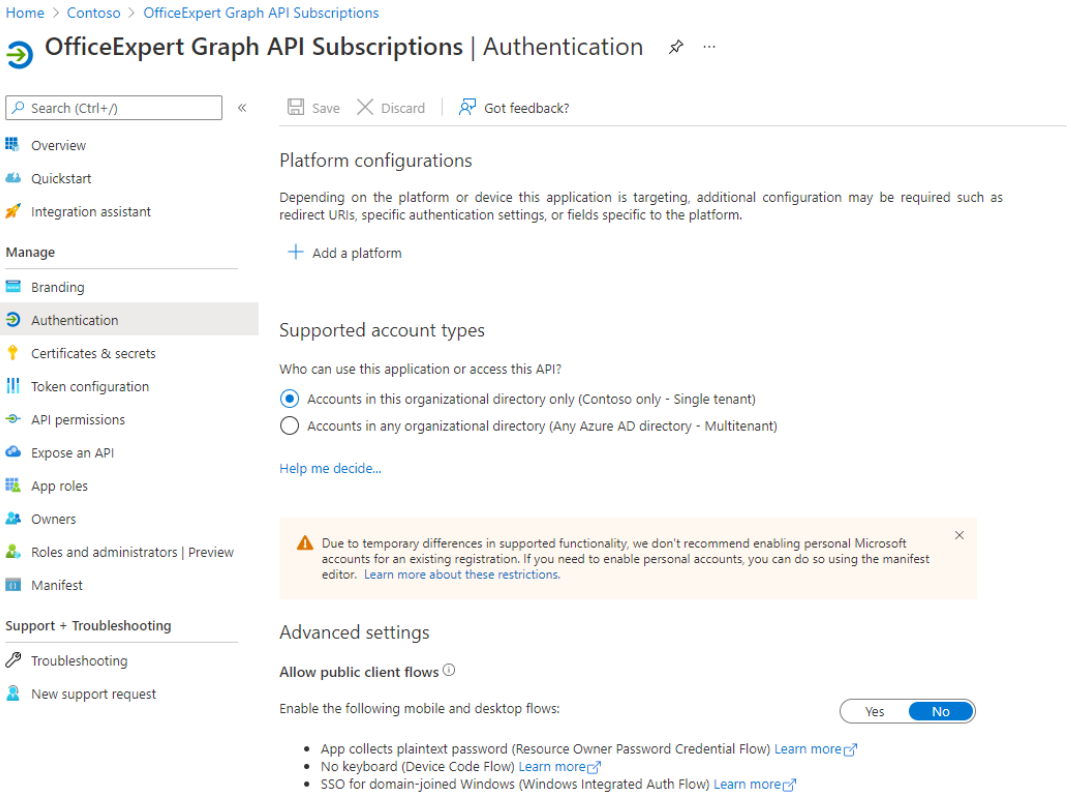
This is a simple single tenant application with all the default settings

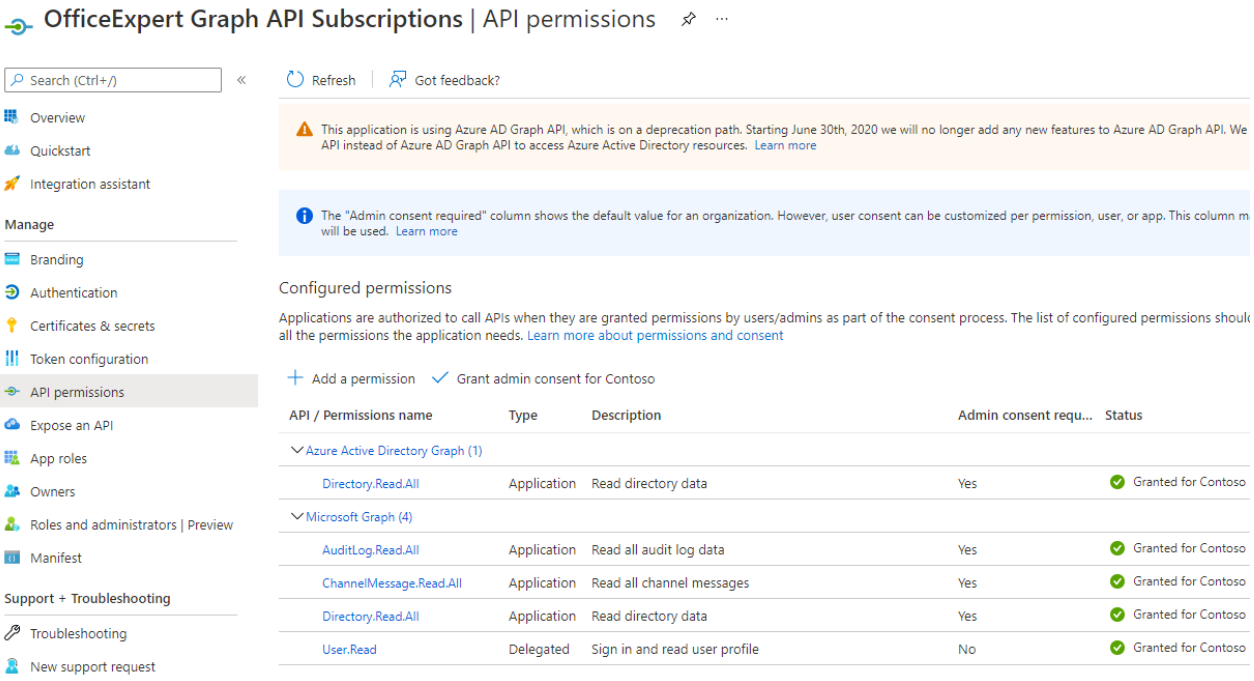
```
1)Create Azure AD App registration -- Name: OfficeExpert Graph API Subscriptions
2)Choose Single Tenant and keep all default settings
3)Open the new registered application and create a client secret (Certificate & secrets)
4)Open the manifest and add the following resource access configuration

"requiredResourceAccess": [
        {
            "resourceAppId": "00000003-0000-0000-c000-000000000000",
            "resourceAccess": [
                {
                    "id": "b0afded3-3588-46d8-8b3d-9842eff778da",
                    "type": "Role"
                },
                {
                    "id": "7b2449af-6ccd-4f4d-9f78-e550c193f0d1",
                    "type": "Role"
                },
                {
                    "id": "7ab1d382-f21e-4acd-a863-ba3e13f7da61",
                    "type": "Role"
                },
                {
                    "id": "e1fe6dd8-ba31-4d61-89e7-88639da4683d",
                    "type": "Scope"
                }
            ]
        },
        {
            "resourceAppId": "00000002-0000-0000-c000-000000000000",
            "resourceAccess": [
                {
                    "id": "5778995a-e1bf-45b8-affa-663a9f3f4d04",
                    "type": "Role"
                }
            ]
        }
    ],

5) Give Admin consent to all the added permissions
```

This should be the final result:



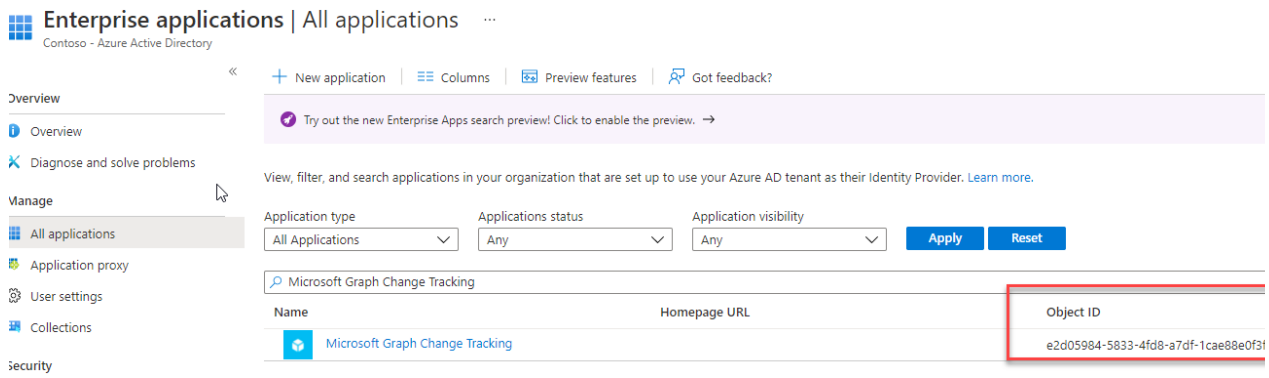


Microsoft Graph Change Tracking Object Id

Perform this within the CSP's Azure tenant!

The Graph Change Tracking Object Id is needed to finalize the deployment.

Open the *Azure Portal* / *Azure AD* / *Enterprise Application* and search for **Microsoft Graph Change Tracking**



Key Vault Access App Registration

Perform this within the CSP's Azure tenant!

In the azure tenant of the CSP , a Azure AD App needs to be registered.

- Name: *panagenda EventHub Key Vault Access - customername*
- Single Tenant
- No permissions
- Create client secret with maximum duration of 24 months

Deployment Information - please provide this to panagenda

Make sure that the OfficeExpert appliance is fully deployed and up and running.

If so, please share the following information with panagenda so that all componentes can be deployed via Azure Lighthouse into your tenant.
Please download the following table as XLSX : https://files.panagenda.com/OfficeExpert/AzureLightHouse/panagenda-azure-light-house-csp.xlsx

Item	Value
Tenant Id of the customer's Microsoft 365 tenant (Customer)	e.g xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
Azure AD App ID of "*OfficeExpert Graph API Subscriptions*" (Customer)	
Client secret of "*OfficeExpert Graph API Subscriptions*" (Customer)	
Tenant Id of the CSP's Azure tenant (CSP)	e.g xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
Primary Domain name of the CSP tenant. Please verify this on your Azure AD properties page (CSP)	e.g. acme.onmicrosoft.com
Key Vault Access App Registration Object Id. (Enterprise applications) (CSP)	
Microsoft Graph Change Tracking Object Id (CSP)	

Azure Location where the components should be deployed (CSP)	 e.g. eastus; westeurope;....
Resource Group Name where the components should be deployed (CSP)	*default*: panagenda-azure-lighthouse
Subscription Id where the components should be deployed (CSP)	
Subscription name where the components should be deployed (CSP)	