

# 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?](#)
- [Deployment Prerequisites](#)
  - [Azure Lighthouse](#)
  - [Graph API Subscription App Registration](#)
  - [Microsoft Graph Change Tracking Object Id](#)
  - [Key Vault Access App Registration](#)
  - [Deployment Information - please provide this to panagenda](#)

## 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.OperationallInsights
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:

## OfficeExpert Graph API Subscriptions | Authentication

Search (Ctrl+/)

Save Discard Got feedback?

- Overview
- Quickstart
- Integration assistant

### Manage

- Branding
- Authentication**
- Certificates & secrets
- Token configuration
- API permissions
- Expose an API
- App roles
- Owners
- Roles and administrators | Preview
- Manifest

### Support + Troubleshooting

- Troubleshooting
- New support request

### Platform configurations

Depending on the platform or device this application is targeting, additional configuration may be required such as redirect URIs, specific authentication settings, or fields specific to the platform.

+ Add a platform

### Supported account types

Who can use this application or access this API?

- Accounts in this organizational directory only (Contoso only - Single tenant)
- Accounts in any organizational directory (Any Azure AD directory - Multitenant)

[Help me decide...](#)

**Due to temporary differences in supported functionality, we don't recommend enabling personal Microsoft accounts for an existing registration. If you need to enable personal accounts, you can do so using the manifest editor. [Learn more about these restrictions.](#)**

### Advanced settings

Allow public client flows

Enable the following mobile and desktop flows:

Yes  No

- App collects plaintext password (Resource Owner Password Credential Flow) [Learn more](#)
- No keyboard (Device Code Flow) [Learn more](#)
- SSO for domain-joined Windows (Windows Integrated Auth Flow) [Learn more](#)

## OfficeExpert Graph API Subscriptions | API permissions

Search (Ctrl+/)

Refresh Got feedback?

- Overview
- Quickstart
- Integration assistant

### Manage

- Branding
- Authentication
- Certificates & secrets
- Token configuration
- API permissions**
- Expose an API
- App roles
- Owners
- Roles and administrators | Preview
- Manifest

### Support + Troubleshooting

- Troubleshooting
- New support request

**This application is using Azure AD Graph API, which is on a deprecation path. Starting June 30th, 2020 we will no longer add any new features to Azure AD Graph API. We will migrate to Microsoft Graph API instead of Azure AD Graph API to access Azure Active Directory resources. [Learn more](#)**

The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column will be used. [Learn more](#)

### Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission  Grant admin consent for Contoso

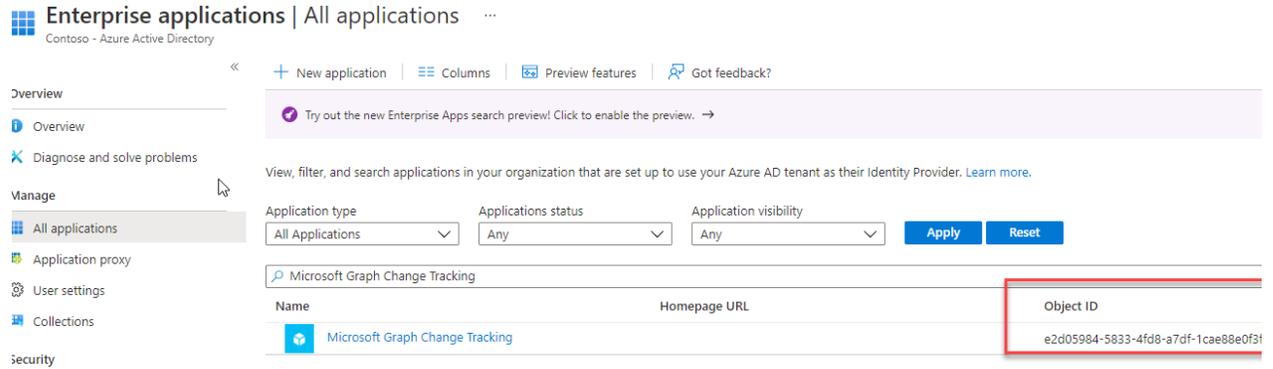
API / Permissions name	Type	Description	Admin consent requ...	Status
Azure Active Directory Graph (1)				
Directory.Read.All	Application	Read directory data	Yes	Granted for Contoso
Microsoft Graph (4)				
AuditLog.Read.All	Application	Read all audit log data	Yes	Granted for Contoso
ChannelMessage.Read.All	Application	Read all channel messages	Yes	Granted for Contoso
Directory.Read.All	Application	Read directory data	Yes	Granted for Contoso
User.Read	Delegated	Sign in and read user profile	No	Granted for Contoso

## 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 componetes 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
<b>Tenant Id</b> of the customer's Microsoft 365 tenant (Customer)	e.g xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
<b>Azure AD App ID</b> of "OfficeExpert Graph API Subscriptions" (Customer)	
<b>Client secret</b> of "OfficeExpert Graph API Subscriptions" (Customer)	
<b>Tenant Id</b> of the CSP's Azure tenant (CSP)	e.g xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
<b>Primary</b> Domain name of the CSP tenant. Please verify this on your Azure AD properties page (CSP)	e.g. <a href="https://acme.onmicrosoft.com">acme.onmicrosoft.com</a>
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)	