



# Customer Portal for Fabric

## Preparation Deployment Guide

Deployment Guide for creation of required resources in Microsoft Entra and Azure tenant.

**Written by:** Ingraphic AS

## Contents

<b>1</b>	<b>INTRODUCTION.....</b>	<b>3</b>
<b>2</b>	<b>ROLES .....</b>	<b>4</b>
<b>3</b>	<b>CHECKLIST .....</b>	<b>4</b>
<b>4</b>	<b>DEPLOYMENT STEPS (BASIC).....</b>	<b>5</b>
4.1	Azure Subscription .....	5
4.1.1	Resource Group.....	6
4.2	Microsoft Entra .....	6
4.2.1	Primary Domain name.....	6
4.3	Entra Groups (Groups Configuration) .....	7
4.4	SQL Configuration .....	8
4.4.1	SQL Server Administrator .....	8
4.4.2	SQL Server Entra Administrator (optional).....	9
4.4.3	Office IP Address (Optional) .....	9
<b>5</b>	<b>ENTRA CONFIGURATION.....</b>	<b>10</b>
5.1	Web Service Principal .....	10
5.2	SPA Service Principal.....	13
5.3	Fabric Service Principal .....	16
5.4	Retrieve Enterprise application Object IDs for SP_Portal- WEB and Fabric .....	17
5.5	Fabric Configuration.....	18
5.5.1	Do you have an existing Fabric Capacity which you would like to use? (optional) .....	19
5.5.2	Name of the existing Fabric Capacity resource (optional) .....	19
5.6	Tags .....	20
<b>6</b>	<b>POST DEPLOYMENT .....</b>	<b>20</b>
6.1	Logic app for e-mail invitations .....	20
<b>7</b>	<b>FAILING APPLICATION.....</b>	<b>21</b>
7.1	Deployment fails .....	21
7.2	Successful deployment, but the application does not work.....	21

## 1 INTRODUCTION

This guide is for technical resources that is responsible for creating the resources needed to deploy the “Portal for Microsoft Fabric” in Microsoft Azure.

The “Portal for Microsoft Fabric will create the following resources during deployment.

Name	Description
Log Analytics Workspace	Collect, analyze and query logs from various Azure services and applications.
Application Insights	Monitoring service that provides real-time performance metrics and analytics, and diagnostics for web applications.
Automation Account	Enables process automation through runbooks, configurations and other features. Used in this case for managing Fabric Capacity Start and Pause schedules.
Runbooks	Workflow scripts in PowerShell that automate Fabric Capacity start up and pause times.
Storage account	Storage for data objects including blobs, files and tables. Used in this case for storing company and logo images, report images and application configuration settings.
SQL Server and Database	Relational database used by the application. Stores user, group, report data and references.
Logic App	Low code workflow automation service which in this case used for automating sending of invite e-mails to external users or customers.
Key Vault	Secure storage for keys, secrets and other credentials. Used by the Container Applications.
Container Apps Environment	Managed hosting environment for containerized applications.

## Fabric Portal – Preparation Deployment Guide

---

Container Instance	Serverless container service that runs isolated containers on-demand. This initializes the database, Fabric Capacity workspace, uploads necessary images and initializes the application.
Container Apps	Managed serverless platform for deploying containerized applications. These are the main components of the frontend and backend parts of this solution.

## 2 ROLES

Roles needed during the preparation of deployment.

Role	Description
<b>Entra Administrator</b>	Entra Administrator role (or corresponding permissions) are needed to create Entra groups and assign users to the groups.
<b>Entra Application Developer</b>	Entra Application Developer role (or corresponding) is needed to create the necessary Service principals and add permissions.
<b>Fabric Administrator</b>	Fabric Administrator role is needed to configure Fabric and add the necessary configurations and settings to the Fabric portal (as shown in section 5.5).
<b>Owner role for Subscription</b>	This is very important to note for the deployment. Due to how Azure Marketplace is setup, only a user with the Owner role at the Subscription level can successfully deploy the application from Azure Marketplace. This is something that needs to be taken into account before deploying the application.

## 3 CHECKLIST

High-level checklist of the steps that is required before the deployment of “Portal for Microsoft Fabric”.

Steps	Description
Entra Primary domain	Primary Domain is used by the Portal Application. This can be found in Microsoft Entra ID.
Entra Groups	Entra Groups are essential for access control and management. The following groups must be created – Users, Admins, Fabric Admins in order to run the application.
Entra Application Registrations	Entra Application Registrations, also known as Service Principals are essential for the application to run, and handles permissions, authentication, authorization and access to various resources. For this application 3 Service Principals are needed – WEB, SPA and Fabric.
Fabric Capacity	Fabric Capacity is used to access, manage and embed Fabric resources like workspaces, reports and dashboards.

## 4 DEPLOYMENT STEPS (BASIC)

### 4.1 Azure Subscription

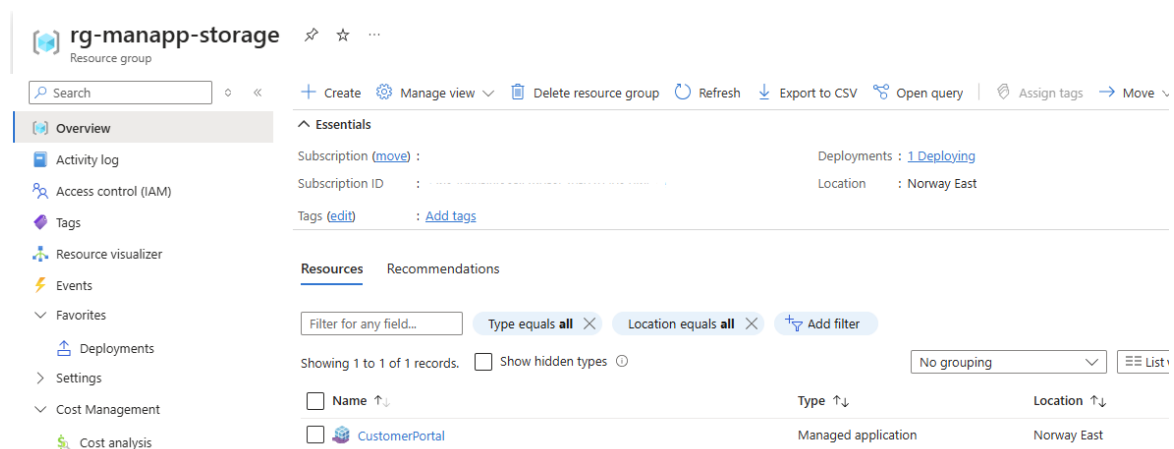
Make sure you have a valid Microsoft Azure subscription ready to be used for the Portal for Fabric Deployment. The Managed Application and resources that follow will be deployed to this subscription.

### 4.1.1 Resource Group

During the deployment in Azure a Resource group is needed to contain the Managed Application resource, which will then be automatically used to build all the Azure resources needed to run the application.

The resource group can be created before the deployment or during the deployment. As mentioned above, this resource group will only contain the Managed Application resource. All other resources that are needed to run the application will be deployed to a separate Managed Resource Group.

Recommended name: **rg-manapp-storage**



The screenshot displays the Azure portal interface for the resource group 'rg-manapp-storage'. The left sidebar shows the navigation menu with 'Overview' selected. The main content area is divided into 'Essentials' and 'Resources' sections. The 'Essentials' section shows the subscription ID, location (Norway East), and deployment status (1 Deploying). The 'Resources' section shows a table with one resource: 'CustomerPortal' of type 'Managed application' located in 'Norway East'.

Name	Type	Location
CustomerPortal	Managed application	Norway East

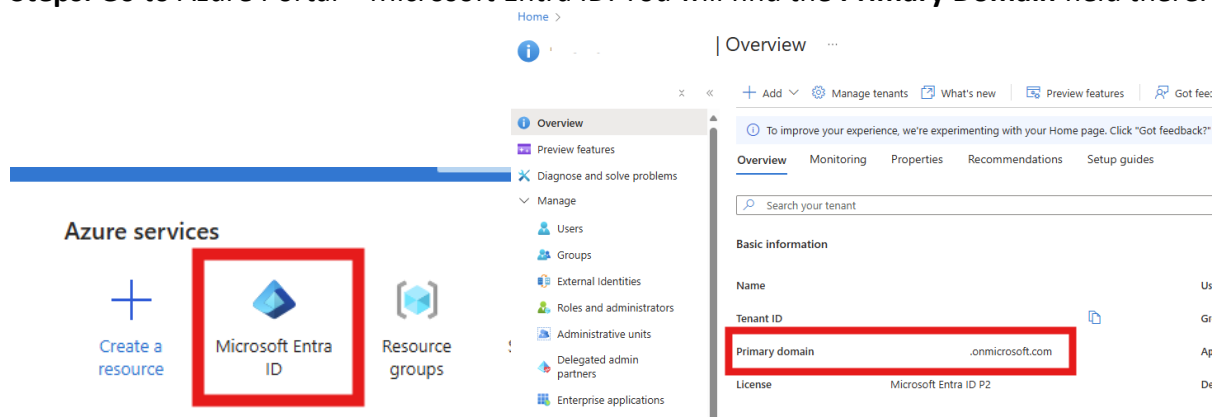
## 4.2 Microsoft Entra

### 4.2.1 Primary Domain name

## Fabric Portal – Preparation Deployment Guide

The primary domain name is needed during the deployment of the Portal for Microsoft Fabric. The domain name can be found here.

**Steps:** Go to Azure Portal – Microsoft Entra ID. You will find the **Primary Domain** field there.



### 4.3 Entra Groups (Groups Configuration)

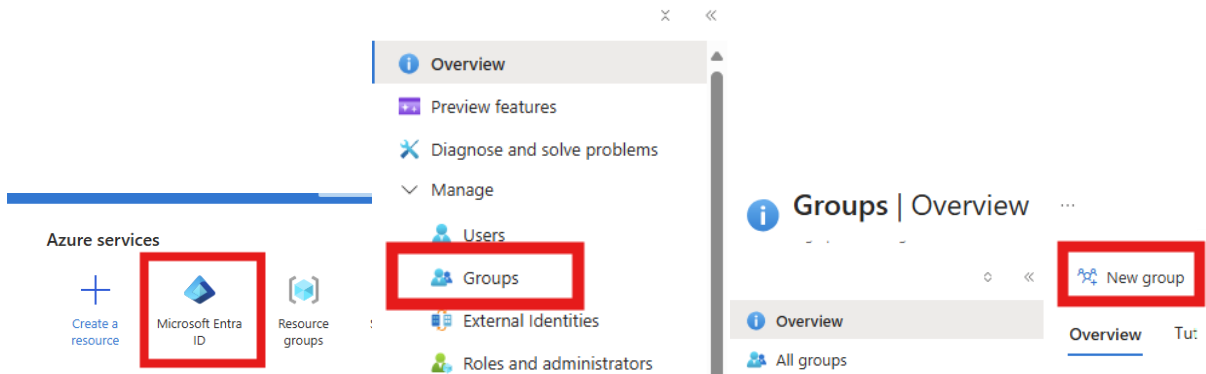
Create new groups that will be used

Group Name	Description
------------	-------------

## Fabric Portal – Preparation Deployment Guide

Portal User Group	Allows access to the Portal as user. Users added to this group will have access to the Portal application and will be able to interact with and navigate through the application. Users have limited permissions, and may not add, edit or remove any existing components. Suggested name for the Entra Group: <b>SG_APP_{Company Standard}_Portal_Users</b>
Portal Admin Group	Allows access to the Portal as admin. Users added to this group have access to the platform, as well as having privileged permissions in the Portal application. Admins may invite new users, create groups, add reports, remove, edit and customize existing configuration and components. Suggested name for the Entra Group: <b>SG_APP_{Company Standard}_Portal_Admins</b>
Fabric Workspace Admin Group	Access to all workspaces created in the Portal application. This group sets the Admins and Owners of the newly created Fabric Workspaces. Suggested name for the Entra Group: <b>SG_APP_{Company Standard}_Portal_FabricAdmins</b>

1. Go to Azure Portal – Microsoft Entra ID – Groups – Add New Group



2. Create the required groups as mentioned in the table above.
3. Assign users to the groups.
4. Do this for all groups.

## 4.4 SQL Configuration

### 4.4.1 SQL Server Administrator

SQL Server Administrator details are used for basic authentication to the database. These fields allow Administrators to login to the SQL Server and database only using Username and Password, without requiring any additional credentials. The SQL Server has strict password requirements, so make sure to make the password hard and unique.



#### 4.4.1.1 Username

The SQL Server Administrator username may only contain lowercase and uppercase letters as well as numbers. Username must NOT start with numbers or symbols.

#### 4.4.1.2 Password

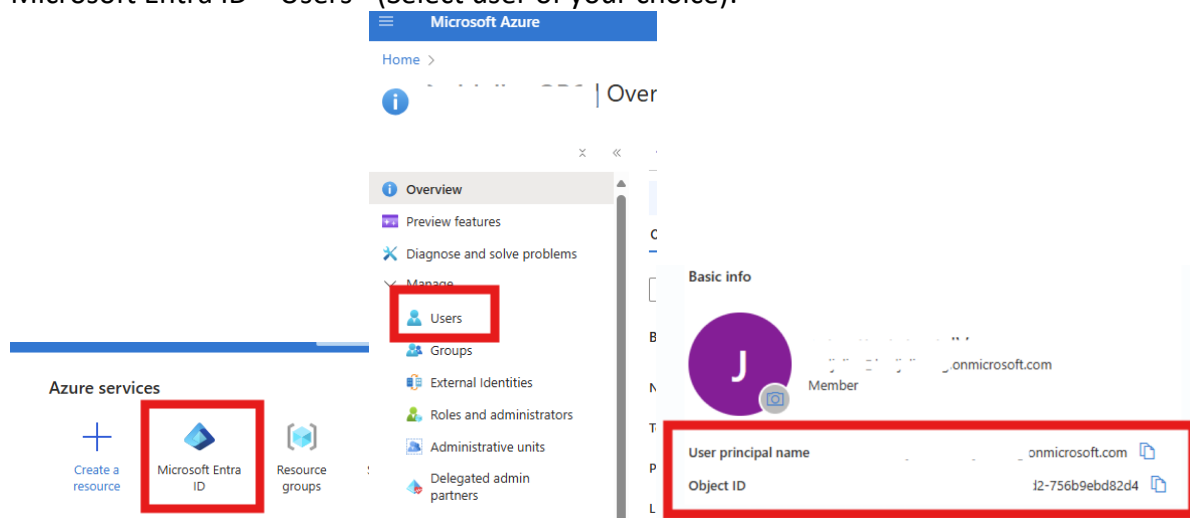
The password must be at least 8 characters in length, but no longer than 128 characters. Password must contain uppercase and lowercase letters, numbers and symbols. Example for a password: **P@ssw0rd1234!** (Don't use this!).

#### 4.4.2 SQL Server Entra Administrator (optional)

These fields are optional but allows you to configure the SQL Server to accept Administrator logins using Entra Authentication as well, which is a more robust and secure solution than basic authentication.

##### 4.4.2.1 Add Entra user as SQL Server Administrator (optional) (4.4.3.1)

For this you will need to provide the UPN (User principal name) and Object ID of the Entra user you want to be Administrator for this SQL Server. These values can be found in Microsoft Entra ID – Users - (Select user of your choice):



#### 4.4.3 Office IP Address (Optional)

Office IP Address is needed for configuration of the SQL Server, for manual access to the database. Azure resources have access by default, but in order to manually access the SQL Database by Administrator, the Office IP address needs to be provided. This step is optional, can be skipped and configured later if necessary or needed, as it won't affect the application in any way.

##### Steps:

1. The easiest way to find the IP Address is to visit: [What Is My IP Address - See Your Public Address - IPv4 & IPv6](#)

2. Copy the IPv4 field.

## 5 ENTRA CONFIGURATION

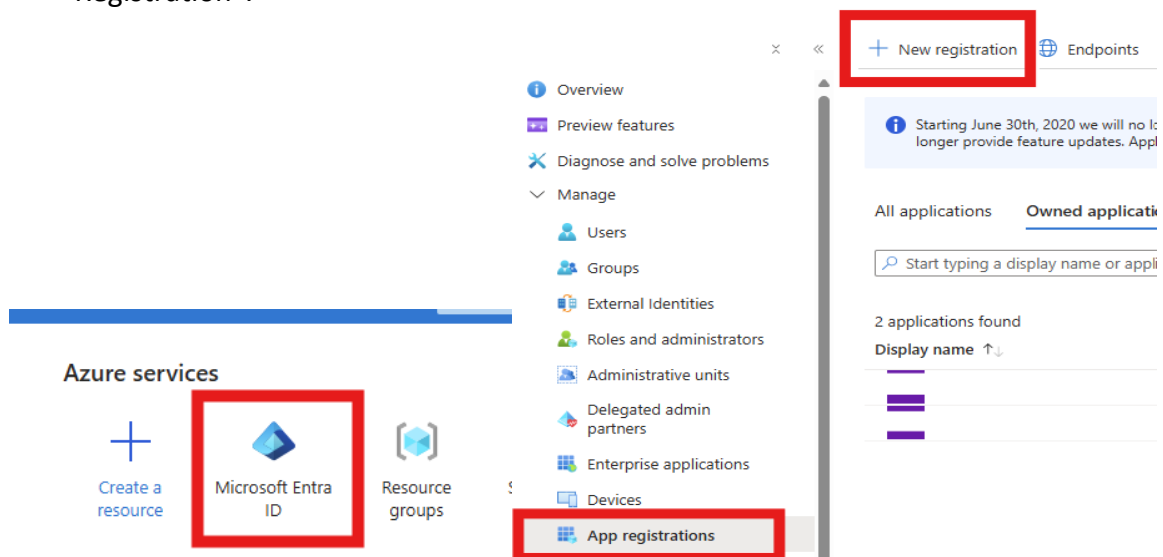
These steps are related to the creation and configuration of Azure Entra Application Registrations, better known as Service Principles. Service principles are used to manage authentication and authorization to the application and different resources, as well as secure access to said resources. These are essential to the Portal application and must be configured correctly.

### 5.1 Web Service Principal

Create Entra Application for back-end. It serves as an identity for the application's backend service when they need to interact with various Azure resources and services. It allows the backend API to authenticate and authorize with Azure Entra, enables for non-interactive and secure access to different resources.

#### Steps :

1. Go to Azure Portal – Microsoft Entra ID – App Registrations. Click on “New Registration”.



2. Give it a name. Suggested name: **SP\_Portal\_WEB** or choose your own.
3. Leave the rest of the configuration as is. Click on “Register”.
4. After the App Registration is created, go to “Certificates & Secrets”, create a new secret and set the expiration time to 730 days. Copy the **Value** of the secret and save it somewhere for later use.

## Fabric Portal – Preparation Deployment Guide

The screenshot shows the Azure portal interface. On the left, the 'Certificates & secrets' blade is selected under the 'Manage' section. In the center, the 'Add a client secret' dialog is open. The 'Description' field is set to 'Portal\_Secret' and the 'Expires' dropdown is set to '730 days (24 months)'. Below the dialog, a table lists the client secrets.

Description	Expires	Value
Portal_Secret	3/14/2027	o-K8Q~1z08Ag3nIWVXcU_b3x~H...

5. In the “API Permissions” blade, add the following permissions:
- Click on “Add a permission”. Then select **Microsoft Graph - Application permissions**:

The screenshot shows the Azure portal interface. On the left, the 'API permissions' blade is selected under the 'Manage' section. In the center, the 'Request API permissions' dialog is open. The 'Microsoft Graph' API is selected, and the 'Application permissions' tab is active. The 'Add permissions' button is highlighted.

- Select the following permissions: **Application.ReadWrite.All, Group.Create, Group.ReadWrite.All, User.Invite.All, User.Read, User.ReadWrite.All**
- Then click **Grant admin consent for <tenant name>**
- Make sure you have these permissions enabled for SP\_Portal\_WEB:

## Fabric Portal – Preparation Deployment Guide

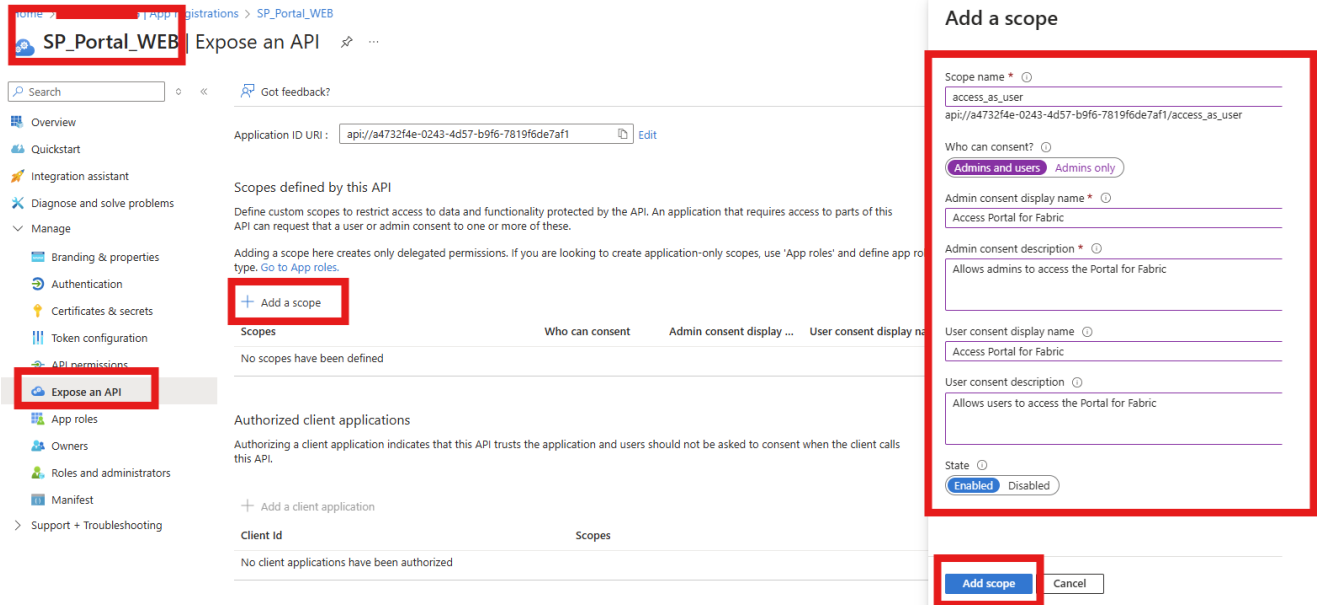
API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (6)				
<a href="#">Application.ReadWrite.All</a>	Application	Read and write all applications	Yes	✓ Granted for
<a href="#">Group.Create</a>	Application	Create groups	Yes	✓ Granted for
<a href="#">Group.ReadWrite.All</a>	Application	Read and write all groups	Yes	✓ Granted for
<a href="#">User.Invite.All</a>	Application	Invite guest users to the organization	Yes	✓ Granted for
<a href="#">User.Read</a>	Delegated	Sign in and read user profile	No	✓ Granted for
<a href="#">User.ReadWrite.All</a>	Application	Read and write all users' full profiles	Yes	✓ Granted for

6. In the “Expose an API” blade, click on “Add a scope”, then an automatically generated URI will appear, click on “Save and continue” and then configure the following:

- Scope Name: access\_as\_user
- Who can consent? Admins and users
- Admin consent display name: Access Portal for Fabric
- Admin consent description: Allows admins to access the Portal for Fabric
- User consent display name: Access Portal for Fabric
- User consent description: Allows users to access the Portal for Fabric

The screenshot shows the Azure portal interface for configuring an API. The left sidebar shows the navigation menu with 'Expose an API' selected. The main pane shows the 'Expose an API' configuration for 'SP\_Portal\_WEB'. The 'Application ID URI' section has an 'Add' button highlighted. The 'Edit application ID URI' pane on the right shows a generated URI: 'api://a4732f4e-0243-4d57-b9f6-7819f6de7af1'. The 'Save' button is highlighted.

## Fabric Portal – Preparation Deployment Guide



Later, once SPA Service Principal is created, we will add the SPA Service Principal as Authorized Client Application to create trust between the service principals.

Copy the Application (client) ID (found in the Overview blade) and Secret value to the required fields in the deployment window. The Enterprise Object ID will be retrieved later in this guide.

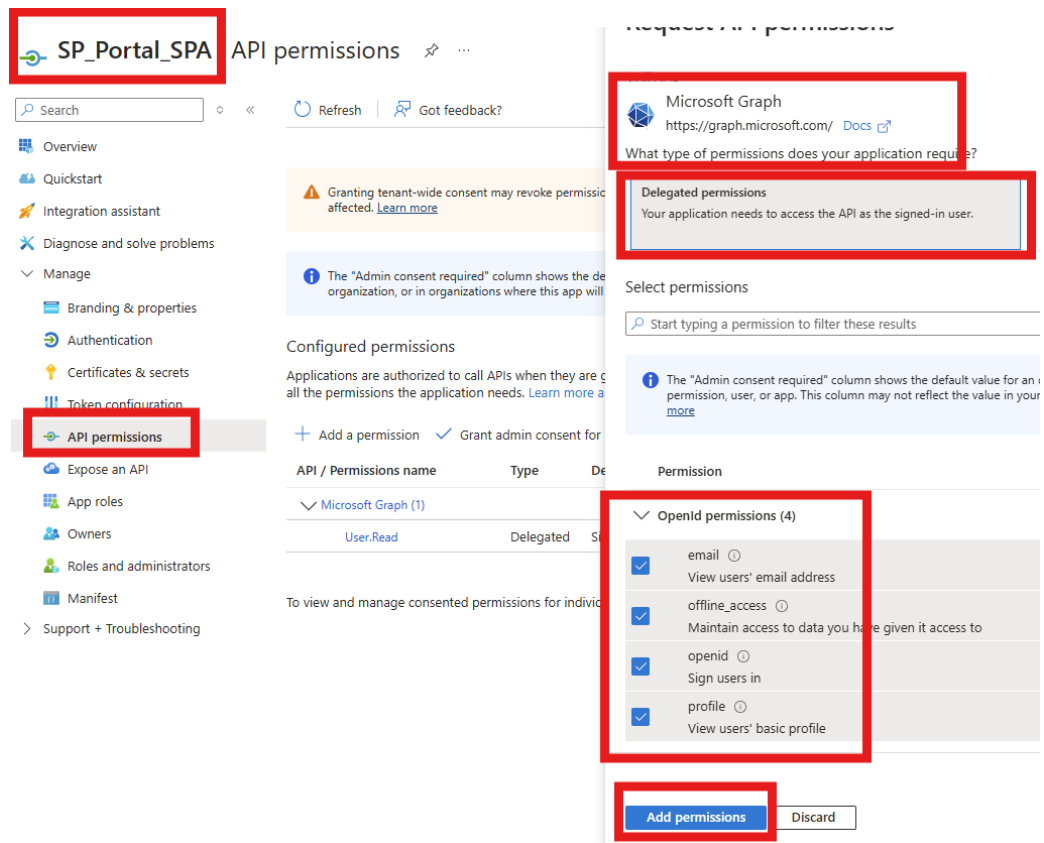
### 5.2 SPA Service Principal

Create Entra Application for front-end. This service principal enables users to sign in to the Portal using Microsoft identity platform. It is a secure way to acquire tokens that are then used to call protected APIs (the backend service of the application).

Steps:

1. Go to Azure Portal – Microsoft Entra ID – App Registrations. Click on “New Registration”.
2. Give it a name. Suggested name: **SP\_Portal\_SPA**
3. In the “API Permissions” blade, add the following permissions: **email, offline\_access, openid, profile, User.Read**


## Fabric Portal – Preparation Deployment Guide



- Also, in “API Permissions” blade, click again on “Add a permission”, the “APIs my organization uses”, then select **SP\_Portal\_WEB – access\_as\_user**.

## Fabric Portal – Preparation Deployment Guide

< All APIs


 SP\_Portal\_WEB  
api://a4732f4e-0243-4d57-b9f6-7819f6de7af1


What type of permissions does your application require?

**Delegated permissions**  
Your application needs to access the API as the signed-in user.

**Application permissions**  
Your application runs as a background service c  
signed-in user.

Select permissions

 Start typing a permission to filter these results

 The "Admin consent required" column shows the default value for an organization. However, user consent can be custo  
permission, user, or app. This column may not reflect the value in your organization, or in organizations where this app  
[more](#)

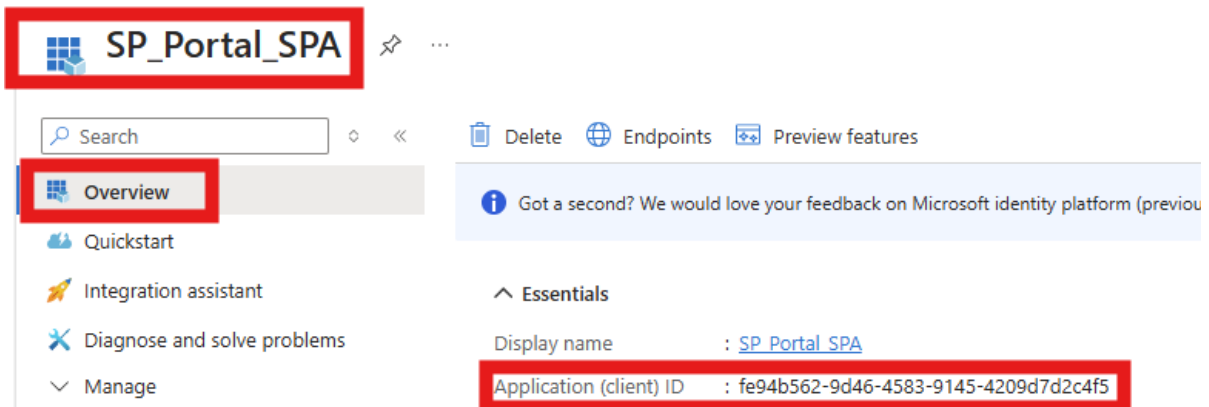
Permission	Admin consent
▼ Permissions (1)	
<input checked="" type="checkbox"/> access_as_user ⓘ Access Portal for Fabric	No

Add permissions

Discard

Lastly, **Grant admin consent**.

Copy the Application (client) ID to the required field in the deployment. The client ID can be found in the **Overview** blade:



Use this same Client ID to add to **SP\_Portal\_WEB – Expose an API – Add client application**. Paste the Client ID and select **Authorized scopes**, then click on **Add application**.

### 5.3 Fabric Service Principal

Create Entra Application for Fabric API Access. Very similar to SP\_CustomerPortal\_WEB. For visual reference and aid, please take a look at section 5.1.

Steps:

1. Go to Azure Portal – **Microsoft Entra ID – App Registrations**. Click on “**New Registration**”.
2. Give it a name. Suggested name: **SP\_Portal\_Fabric**
3. Just like with **SP\_Portal\_WEB** application, after the App Registration is created, go to “**Certificates & Secrets**”, create a new secret and set the expiration time to 730 days. Copy the value of the secret.
4. In the “**API Permissions**” blade, add the following **Delegated** permissions: **PowerBI – Delegated permissions: Capacity.ReadWrite.All, Dashboard.ReadWrite.All, Dataset.ReadWrite.All, PaginatedReport.ReadWrite.All, Report.ReadWrite.All, Workspace.ReadWrite.All** and **Grant Admin Consent**
5. Make sure your newly added permissions look like this:

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 shows all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission    ✓ Grant admin consent for

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (1)				
User.Read	Delegated	Sign in and read user profile	No	✓ Granted for
Power BI Service (6)				
Capacity.ReadWrite.All	Delegated	Read and write all capacities	No	✓ Granted for
Dashboard.ReadWrite.All	Delegated	Make API calls that require read and write permissions on ...	No	✓ Granted for
Dataset.ReadWrite.All	Delegated	Read and write all datasets	No	✓ Granted for
PaginatedReport.ReadWrite.A	Delegated	Make API calls that require read and write permissions on ...	No	✓ Granted for
Report.ReadWrite.All	Delegated	Make API calls that require read and write permissions on ...	No	✓ Granted for
Workspace.ReadWrite.All	Delegated	Read and write all workspaces	No	✓ Granted for

6. Then add this Service Principal to the **SG\_APP\_Portal\_FabricAdmins** Group in **Microsoft Entra – Groups**.

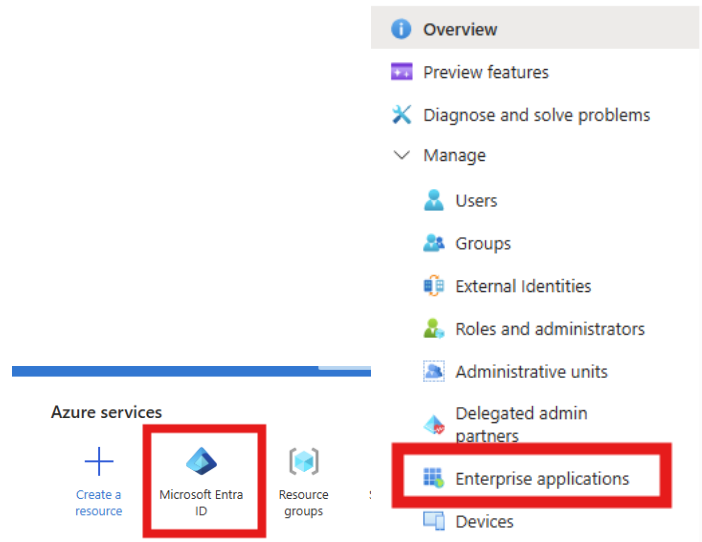
Copy the Client ID and Secret value to the required field in the deployment page. The required Object ID for **SP\_Portal\_Fabric** and **SP\_Portal\_WEB** will be retrieved in the next paragraph.



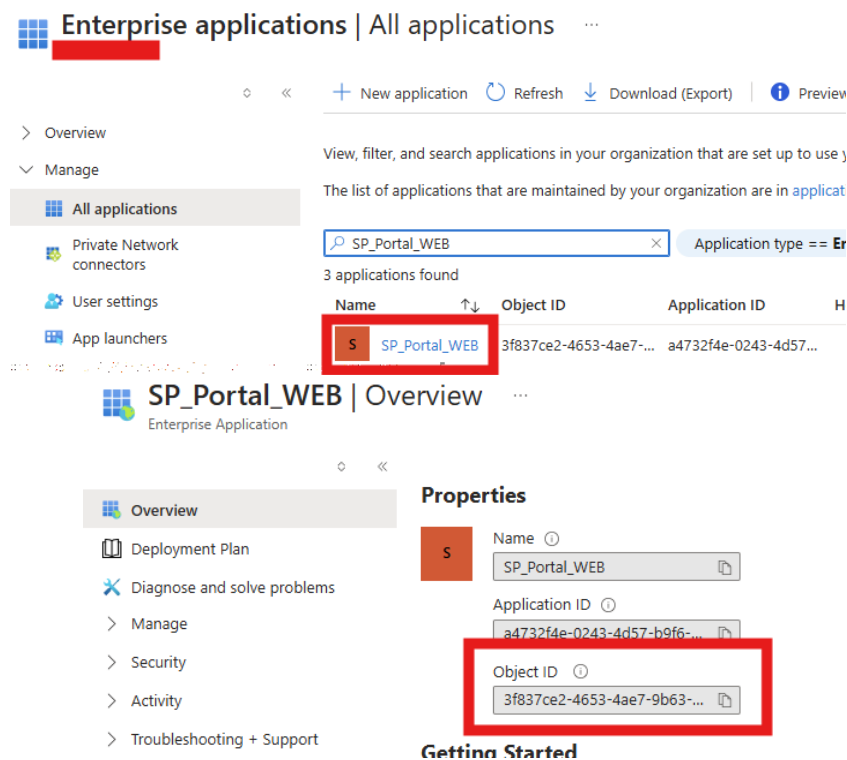
## 5.4 Retrieve Enterprise application Object IDs for SP\_Portal- WEB and Fabric

To retrieve the Enterprise application Object IDs of the **SP\_Portal\_WEB** and **SP\_Portal\_Fabric** service principals, we need to first access the Enterprise Applications blade in Microsoft Entra ID:

1. Go to **Microsoft Entra ID – Enterprise applications**



2. Then search for **SP\_Portal\_WEB** and copy the **Object ID**. Do the same for **SP\_Portal\_Fabric** and paste these values into their corresponding fields in the deployment page:



## 5.5 Fabric Configuration

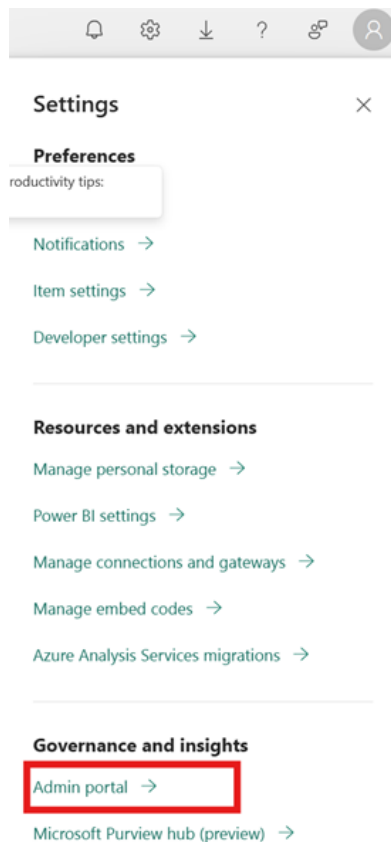
The following input is needed to connect the portal to Microsoft Fabric Capacity that will be used during the deployment.

If you already have an existing Fabric Capacity, you may use that. If not, then a new Capacity must be created, and Trial version can be used.

NOTE: If you don't have an existing Fabric Capacity License and are having troubles with setup of a regular or trial version, please contact us at: [portalsupport@ingraphic.no](mailto:portalsupport@ingraphic.no)

Additionally, several settings must be enabled in Fabric for the solution to work.

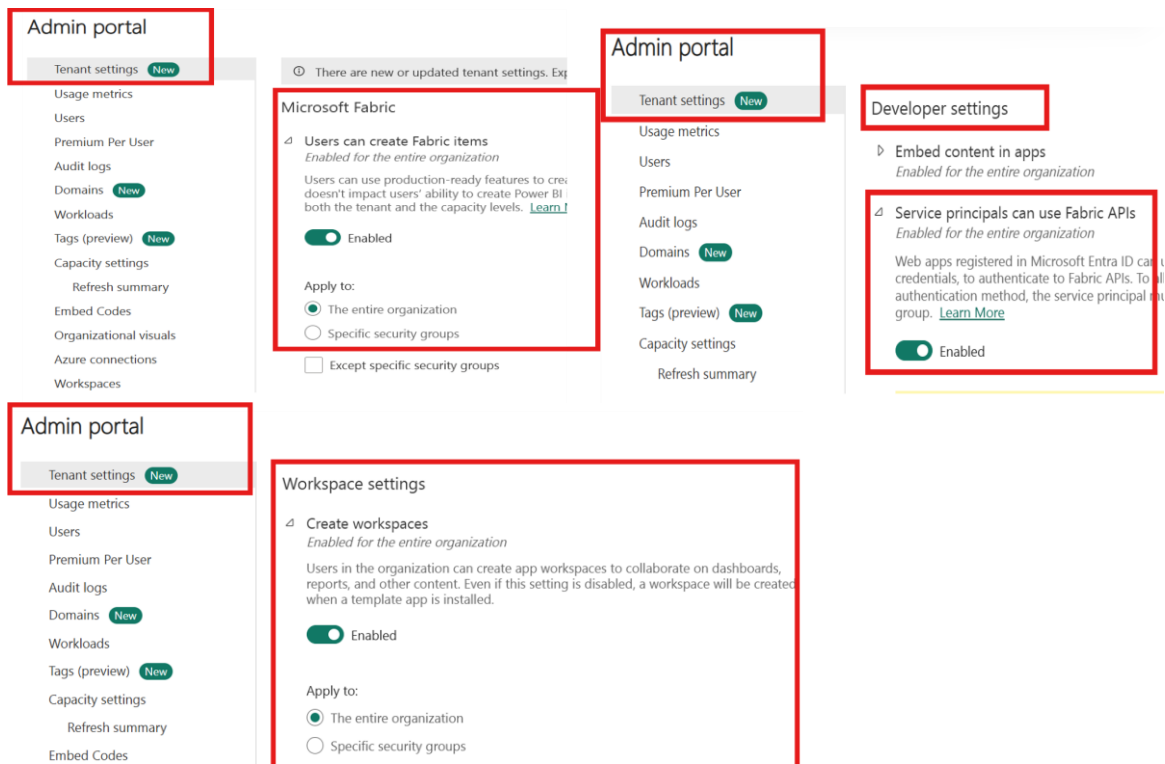
In Fabric, select the gear icon at the top of the page, then select "Admin portal":



In "Tenant settings", enable the following (see below for image reference):

Section	Setting to be enabled
Microsoft Fabric	Users can create Fabric items
Workspace settings	Create workspaces
Developer settings	Service principals can use Fabric APIs

## Fabric Portal – Preparation Deployment Guide



### 5.5.1 Do you have an existing Fabric Capacity which you would like to use? (optional)

This is an optional checkbox to check if you have an already existing Fabric Capacity. If you already have one and would like to use that, please enable this checkbox. And fill the name of the Fabric Capacity resource name into the text field below.

### 5.5.2 Name of the existing Fabric Capacity resource (optional)

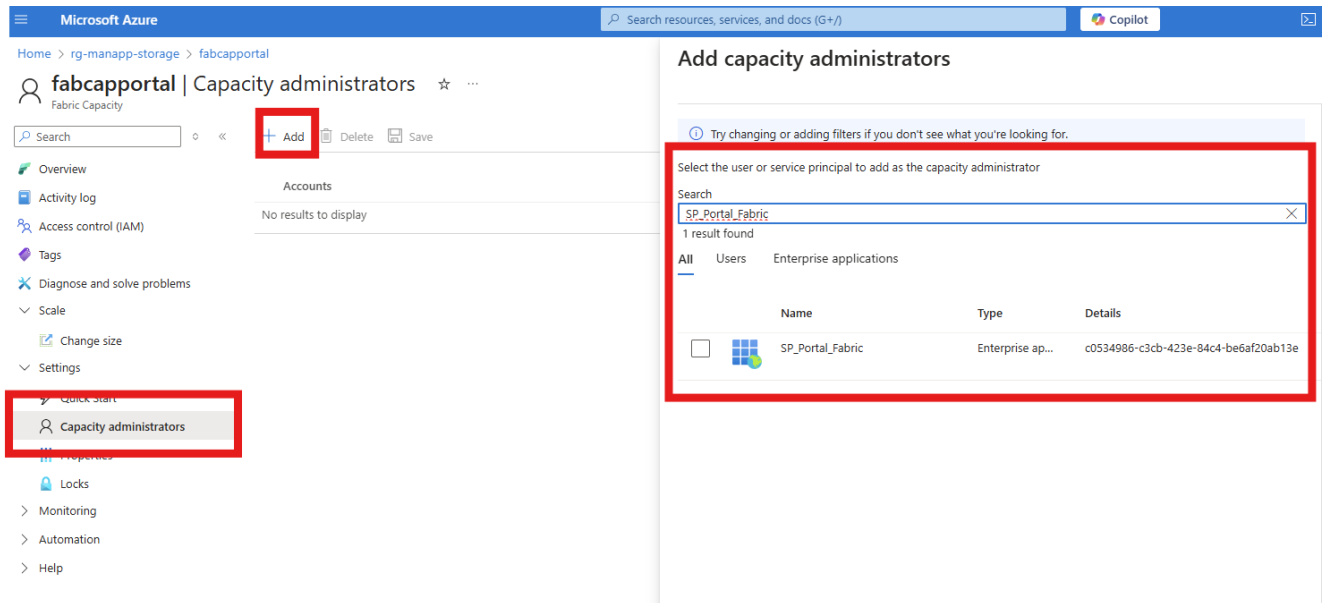
Resource name of the already existing Fabric Capacity resource is required if the above checkbox is checked. The initialization container that sets up the application for use “out of the door” requires the Fabric Capacity resource name in order to retrieve the Capacity License ID.

Please leave this blank if you would like the deployment to create a Fabric Capacity for you.

### IMPORTANT!

If you decide to use your own Fabric Capacity, please add the **SP\_Portal\_Fabric** service principal as **Capacity Administrator** to your existing Fabric Capacity and save:

## Fabric Portal – Preparation Deployment Guide



### 5.6 Tags

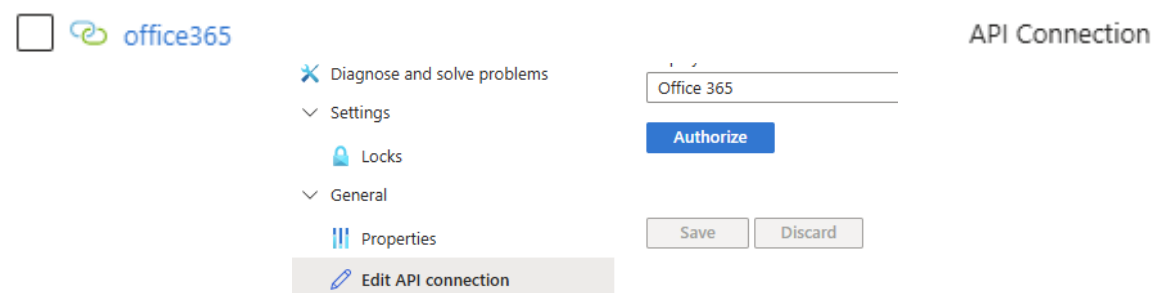
Tags are essential for good organization and resource management in Azure. Good tagging practices allow for easier and better insights and cost management, and helps you categorize resources by department, project or environment.

## 6 POST DEPLOYMENT

There are several minor things that need to be done post deployment for the application to work as expected.

### 6.1 Logic app for e-mail invitations

Logic app is required to send invitation e-mails to new and existing customers. The created Logic app resource uses Outlook messaging system to send e-mails, therefore it must be authenticated. Once deployment is done, please go into the API connection resource called **office 365** and authenticate an e-mail address you want e-mails to be sent from. To authenticate, go to **office 365 – General – Edit API connection – Authorize** and then save.



## 7 FAILING APPLICATION

If the deployment has succeeded, then you can access the application already to confirm that it works. To do so, go to the newly created Resource group and select the frontend container app named **ca-<customername>-cp-front** and click on the URL. If the deployment and initialization is successful, then you will be prompted to sign-in, and after that you will be able to use the application. However, if you were not able to access the application or the application didn't load, please refer to one of the points below.

### 7.1 Deployment fails

If the deployment is failing, please check the error messages presented under deployment. Make sure you have **Owner permissions** at the Subscription level. If any other problems arise, Azure will let you know by showing you an error message. If you need assistance, please contact us.

### 7.2 Successful deployment, but the application does not work

If the deployment succeeded, but the application does not work, please check the Container Instance named initialization-container, then go to Settings – Containers – Logs and check for error messages. The most probable issue is that permissions are not correctly set or Fabric hasn't been configured correctly. Please check the permissions and configurations as explained above.

If you have any problems and/or need assistance, please contact us at:  
[portalsupport@ingraphic.no](mailto:portalsupport@ingraphic.no).