Ingraphic

Customer Portal for Fabric

Preparation Deployment Guide

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

Written by: Ingraphic AS

Owner: Ingraphic AS

Contents

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.

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	Target	Description
Entra Administrator		NEED DESCS FOR ALL
Entra Application Developer		
Fabric Administrator		
RBAC Administrator		

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)

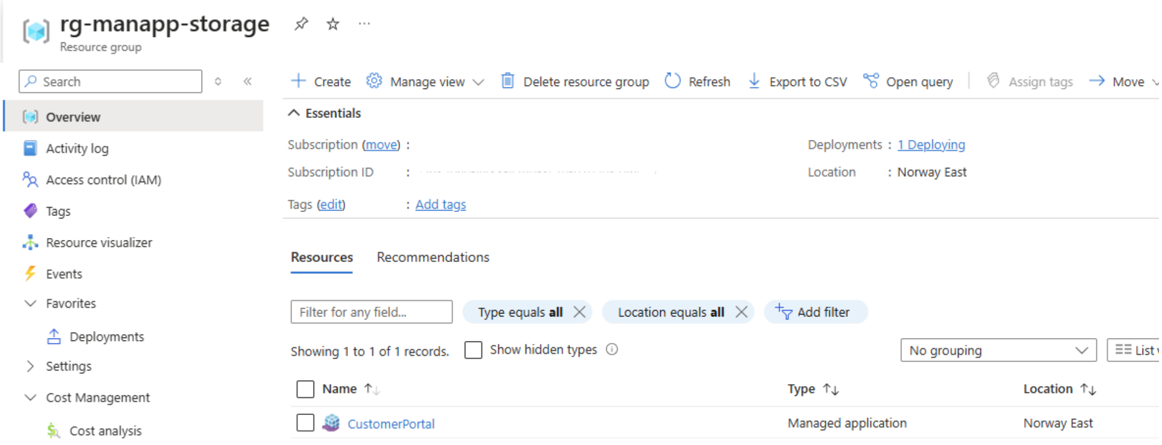
4.1 Azure Subscription

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 seperate Managed Resource Group.

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



Subscription (move) :
Subscription ID : [redacted]
Tags (edit) : Add tags
Deployments : 1 Deploying
Location : Norway East

Showing 1 to 1 of 1 records.

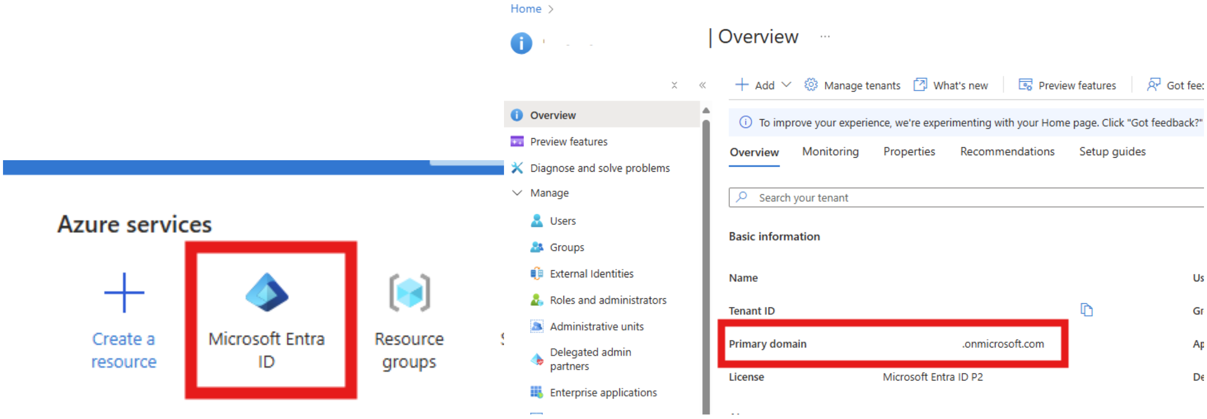
Name	Type	Location
CustomerPortal	Managed application	Norway East

4.2 Microsoft Entra

4.2.1 Primary Domain name

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.



To improve your experience, we're experimenting with your Home page. Click "Got feedback?"

Basic information

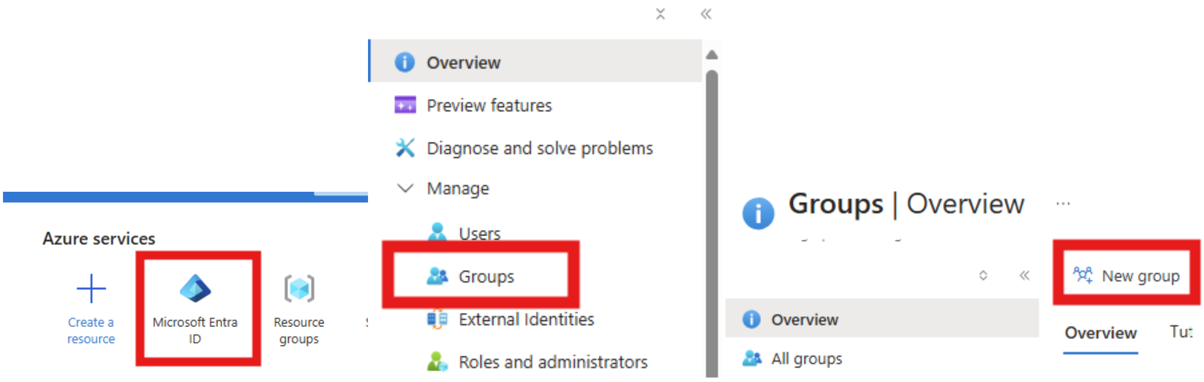
Name	
Tenant ID	
Primary domain	.onmicrosoft.com
License	Microsoft Entra ID P2

4.3 Entra Groups (Groups Configuration)

Create new groups that will be used

Group Name	Description
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: **SG_APP_{Company Standard}_Portal_Users**
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: **SG_APP_{Company Standard}_Portal_Admins**
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: **SG_APP_{Company Standard}_Portal_FabricAdmins**

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

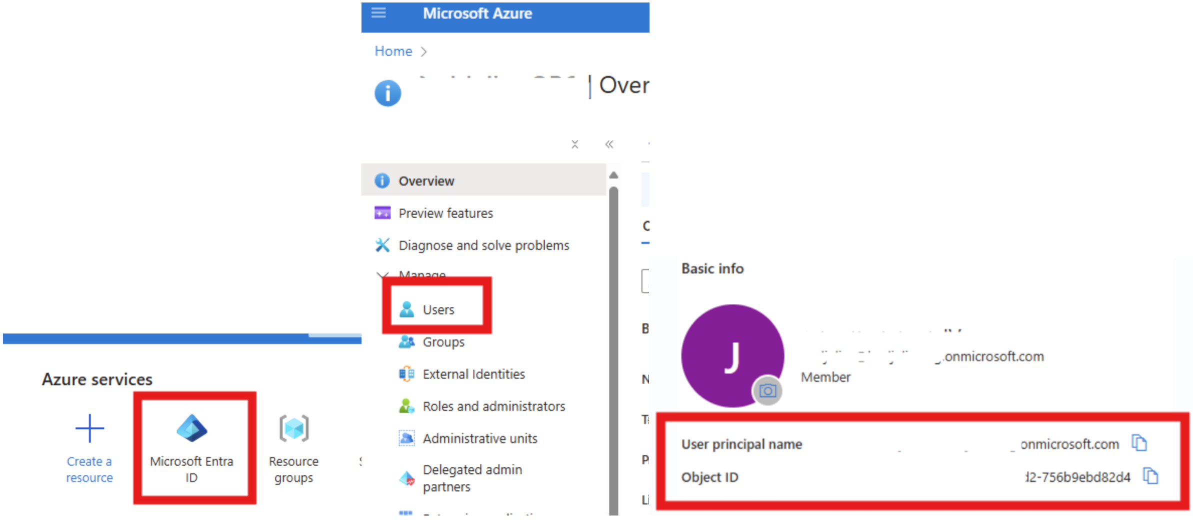
The password must be at least 8 characters in length, but no longer than 128 characters. Password must contain uppercase and lowercase letters, numbers and symbols. Example for a password: **P@ssw0rd1234!**

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):



User principal name onmicrosoft.com
Object ID d2-756b9ebd82d4

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 access the SQL Server by Administrator, the Office IP address needs to be provided manually. This step is optional, can be skipped and configured later if necessary.

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

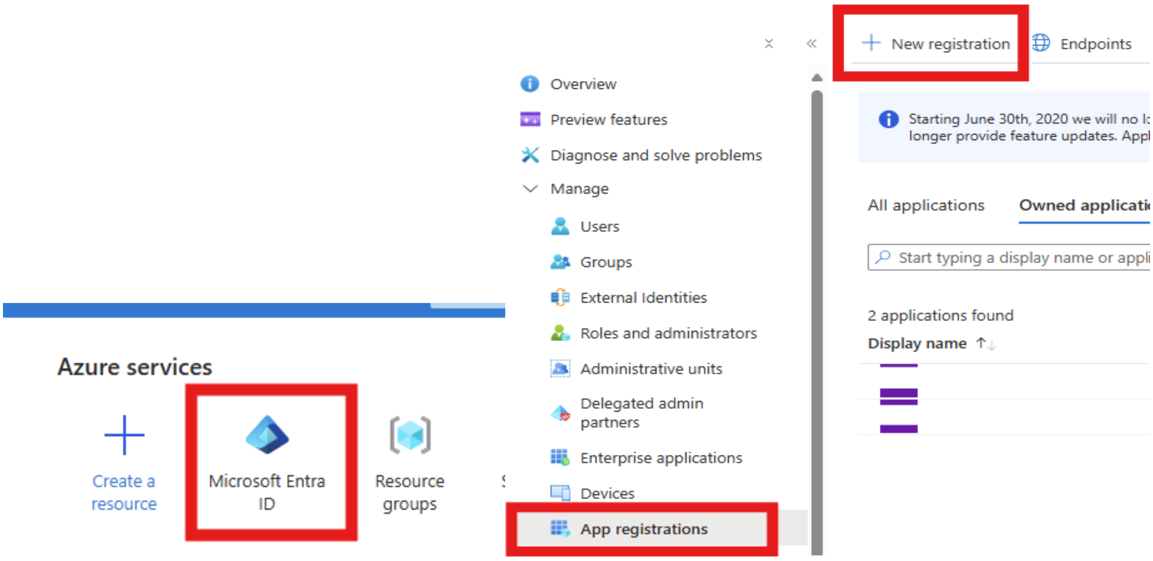
These steps are related to the creation and configuration of Azure Entra Application Registrations, better known as Service Principles. Service principles are used to manage authentication and authorization to the application and different resources, as well as secure access to said resources. These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

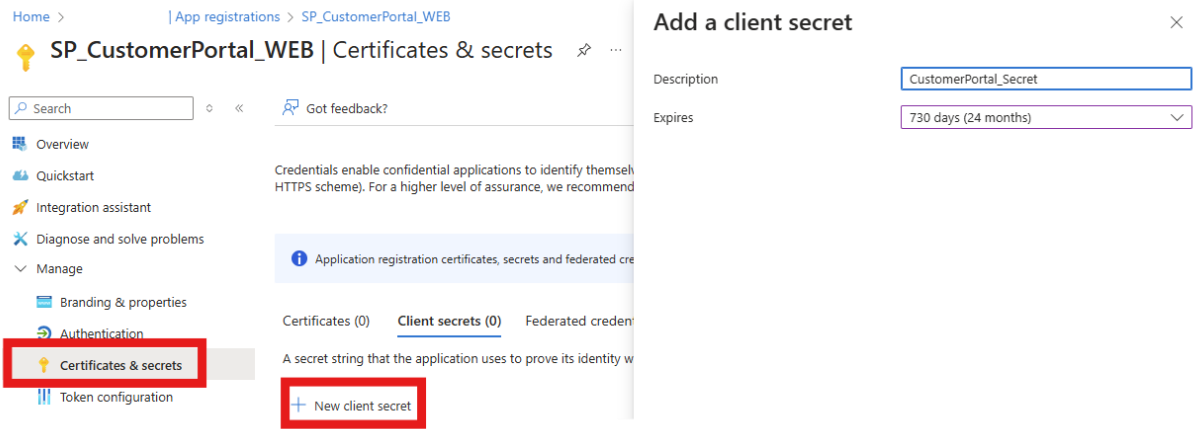
1. Go to Azure Portal – Microsoft Entra ID – App Registrations. Click on “New Registration”.



Starting June 30th, 2020 we will no l
longer provide feature updates. Appl

2 applications found

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.



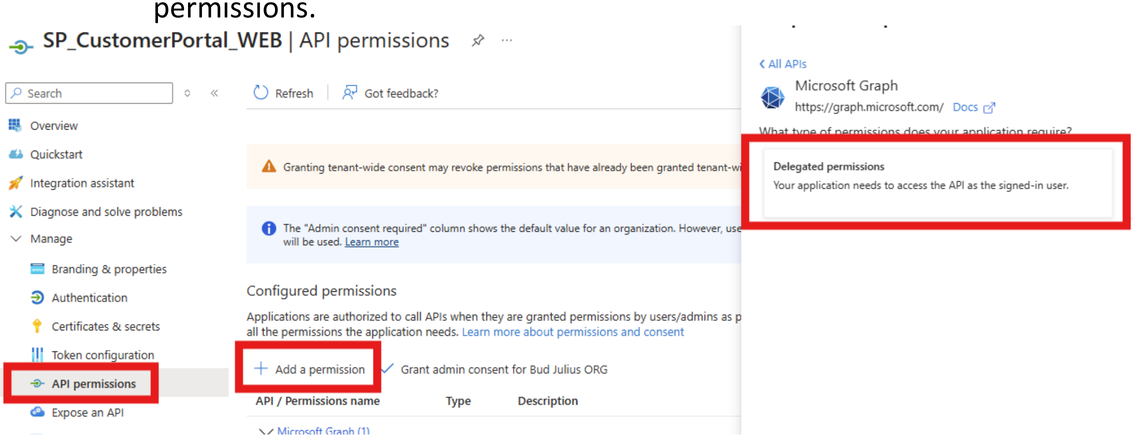
Credentials enable confidential applications to identify themsel
HTTPS scheme). For a higher level of assurance, we recommend

Application registration certificates, secrets and federated cre

A secret string that the application uses to prove its identity w

Description: CustomerPortal_Secret
Expires: 730 days (24 months)

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



Granting tenant-wide consent may revoke permissions that have already been granted tenant-wi

The "Admin consent required" column shows the default value for an organization. However, use
will be used. Learn more

Configured permissions

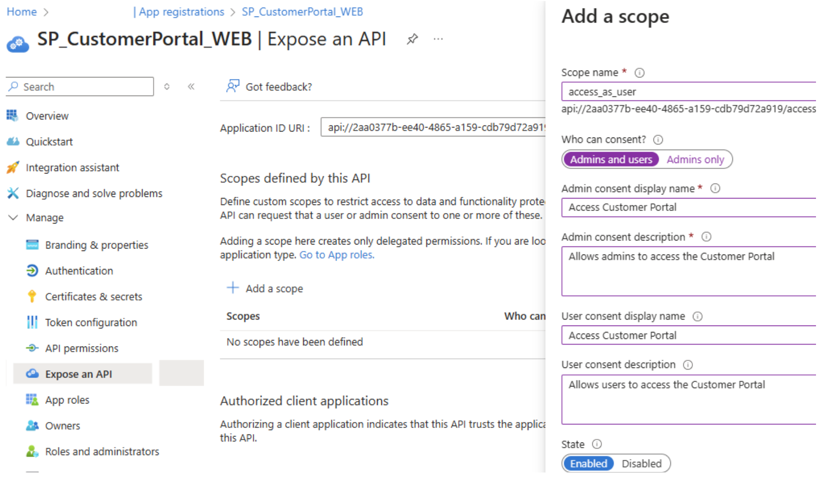
Applications are authorized to call APIs when they are granted permissions by users/admins as p
all the permissions the application needs. Learn more about permissions and consent

What type of permissions does your application require?

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

   - Select the following permissions: **Group.Create, Group.ReadWrite.All, User.Invite.All, User.Read, User.ReadWrite.All**

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 Customer Portal
    - Admin consent display name: Access Customer Portal
    - User consent display name: Access Customer Portal
    - User consent description: Allows users to access the Customer Portal



Application ID URI : api://2aa0377b-ee40-4865-a159-cdb79d72a91

Scopes defined by this API

Define custom scopes to restrict access to data and functionality prote
API can request that a user or admin consent to one or more of these.

Adding a scope here creates only delegated permissions. If you are loo
application type. Go to App roles.

No scopes have been defined

Authorized client applications

Authorizing a client application indicates that this API trusts the applica
this API.

Add a scope

Scope name * : access_as_user
api://2aa0377b-ee40-4865-a159-cdb79d72a919/access

Who can consent? [✓ Admins and users] Admins only

Admin consent display name * : Access Customer Portal

Admin consent description * : Allows admins to access the Customer Portal

User consent display name : Access Customer Portal

User consent description : Allows users to access the Customer Portal

State [✓ Enabled] Disabled

7. Later, once SPA Service Principal is created, we will add the SPA Service Principal as Authorized Client Application.

Copy the Application (client) ID and Secret value to the required fields.

5.2 SPA Service Principal

Create Entra Application for front-end. (DESCRIPTION).

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**
4. Also, in “API Permissions” blade, click again on “Add a permission”, the “My APIs”, then select SP_CustomerPortal_WEB – access_as_user

Copy the Client ID to the required field.

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.

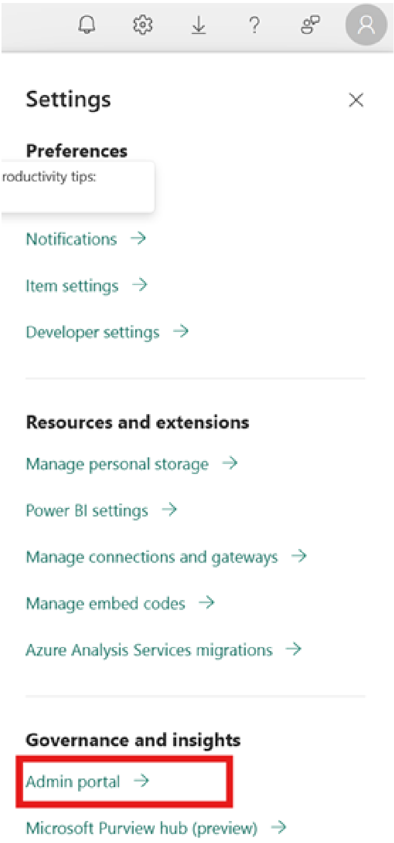
Steps:

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. 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 permissions: PowerBI – Delegated: **Capacity.ReadWrite.All, Dashboard.ReadWrite.All, Dataset, Read.Write.All, Report.Read.Write.All, Workspace.ReadWrite.All** and **Grant Admin Consent**
5. Then add this Service Principal to the SG_APP_CustomerPortal_FabricAdmins Group.

Copy the Client ID and Secret value to the required field.

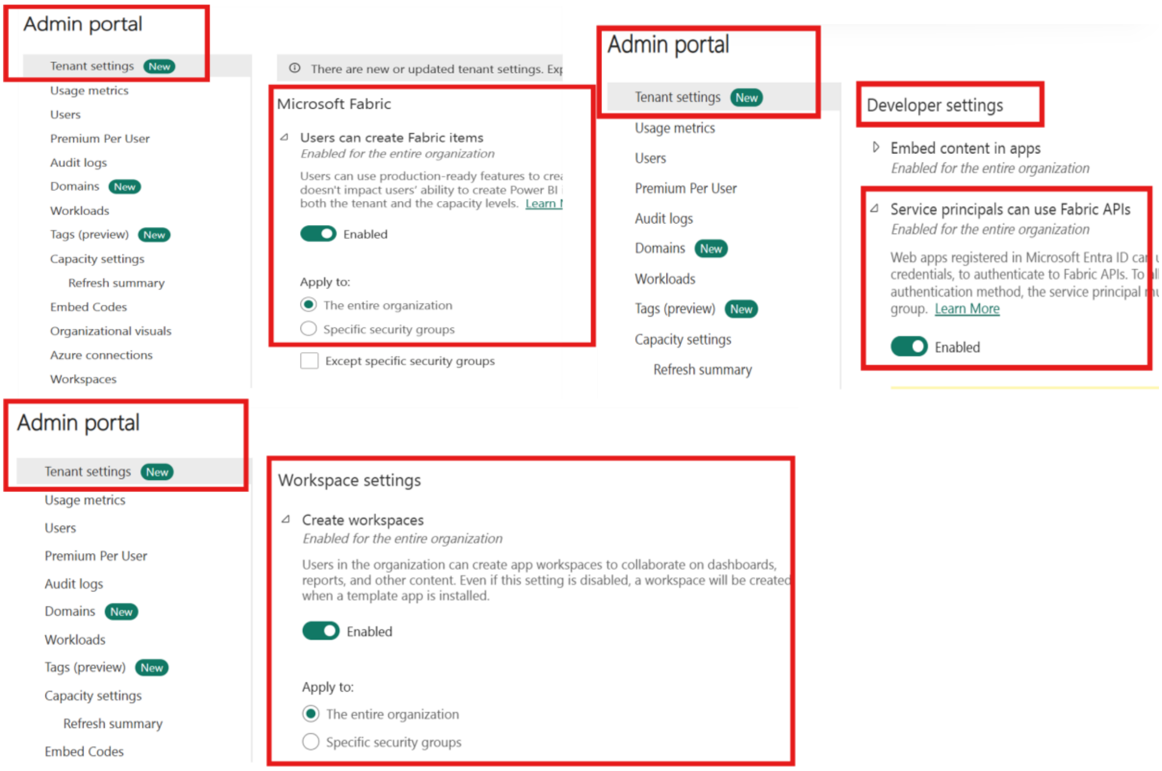
5.4 Microsoft Fabric Configuration

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: info@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



ⓘ There are new or updated tenant settings. Exp

Microsoft Fabric

Users can create Fabric items
Enabled for the entire organization

Users can use production-ready features to crea doesn't impact users' ability to create Power BI both the tenant and the capacity levels. Learn I

Enabled

Apply to:
● The entire organization
○ Specific security groups
□ Except specific security groups

Developer settings

Embed content in apps
Enabled for the entire organization

Service principals can use Fabric APIs
Enabled for the entire organization

Web apps registered in Microsoft Entra ID ca credentials, to authenticate to Fabric APIs. To authentication method, the service principal group. Learn More

Enabled

Workspace settings

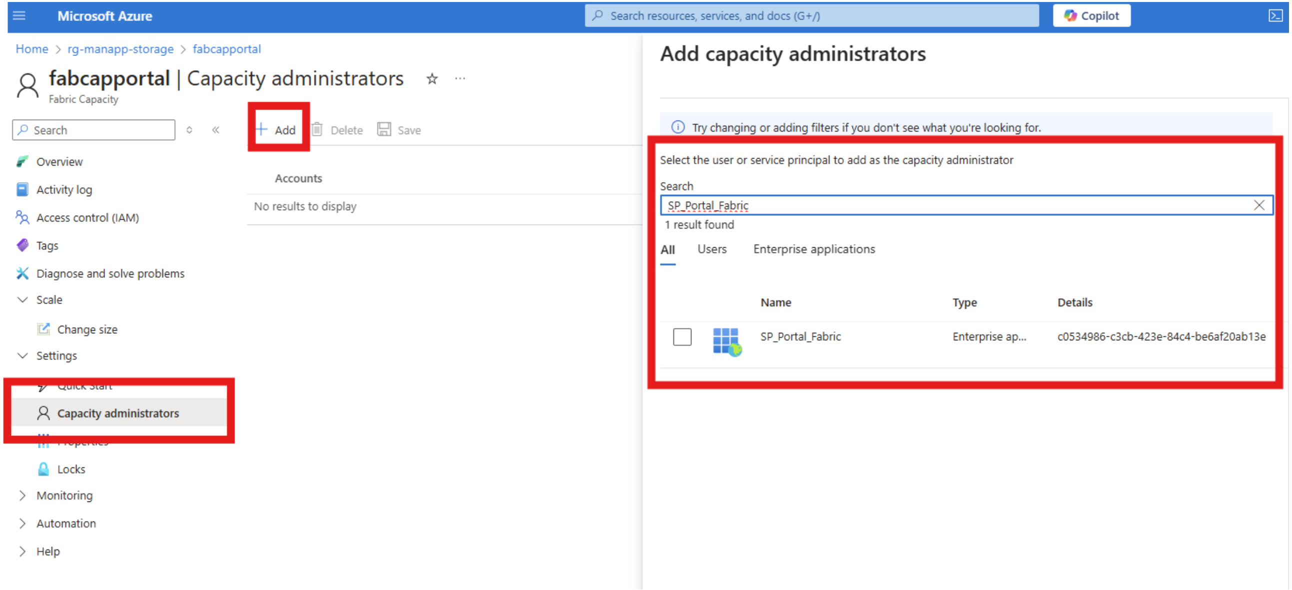
Create workspaces
Enabled for the entire organization

Users in the organization can create app workspaces to collaborate on dashboards, reports, and other content. Even if this setting is disabled, a workspace will be created when a template app is installed.

Enabled

Apply to:
● The entire organization
○ Specific security groups

After this is done, one last step remains for the application to be functional. The Fabric Capacity that has been created, needs to have the Fabric service principal **SP_Portal_Fabric** assigned as administrator. To do this, find the newly created (or existing) Fabric Capacity resource, add the **SP_Portal_Fabric** service principal as **Capacity Administrator** and save:



Accounts
No results to display

Add capacity administrators

ⓘ Try changing or adding filters if you don't see what you're looking for.

Select the user or service principal to add as the capacity administrator

Search: SP_Portal_Fabric

1 result found

All Users Enterprise applications

	Name	Type	Details
□	SP_Portal_Fabric	Enterprise ap...	c0534986-c3cb-423e-84c4-be6af20ab13e

5.4.1 Fabric Capacity ID

Fabric Capacity License ID is used for managing and accessing Fabric resources. The Customer Portal Application uses Fabric to create new workspaces, assign administrators, retrieve and update reports and dashboards, which can then be embedded in the Portal.

To retrieve the Fabric Capacity License ID, do the following:
Steps:

1. Go to Power BI app portal – Admin Portal – Capacity Settings – Click on the gear icon.
2. The Capacity License ID will now appear on the popup blade.

5.4.2 Fabric Capacity Resource Name

Resource name of the already existing Fabric Capacity resource is required.

5.5 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 Logic app resource and authenticate an e-mail address you want e-mails to be sent from.

6.2 Contributor role for SP_CustomerPortal_Deployment

This role has to be assigned to the Deployment Service Principal at the Resource group level, in order to be able to configure Continuous Deployment pipeline and keep your application up-to-date at all times.

6.3 SP_CustomerPortal_SPA

The frontend facing Service Principal also needs Single-Page application Redirect URIs configured. Please go to Microsoft Entra ID – App registrations – SP_CustomerPortal_SPA – Authentication and add the frontend container URI. This will allow the application to redirect users after login.