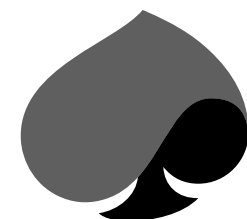


# MCM

## Standardisation des MaaS - Gateway

### Configuration de l'APIM console - Gravitee

21/10/2022



Programme Mon Compte Mobilité, porté par Capgemini et son porteur associé La Fabrique des Mobilités



# Sommaire

1. Prérequis
2. Création des API :
  - 2.1 From scratch
  - 2.2 Depuis une configuration existante
3. Création des Plans
4. Configuration des API
5. Publication de la documentation d'une API
6. Définition des policies sur les API & endpoints
7. Autres configurations

# Prérequis

La configuration de la console APIM Gravitee nécessite certains prérequis :

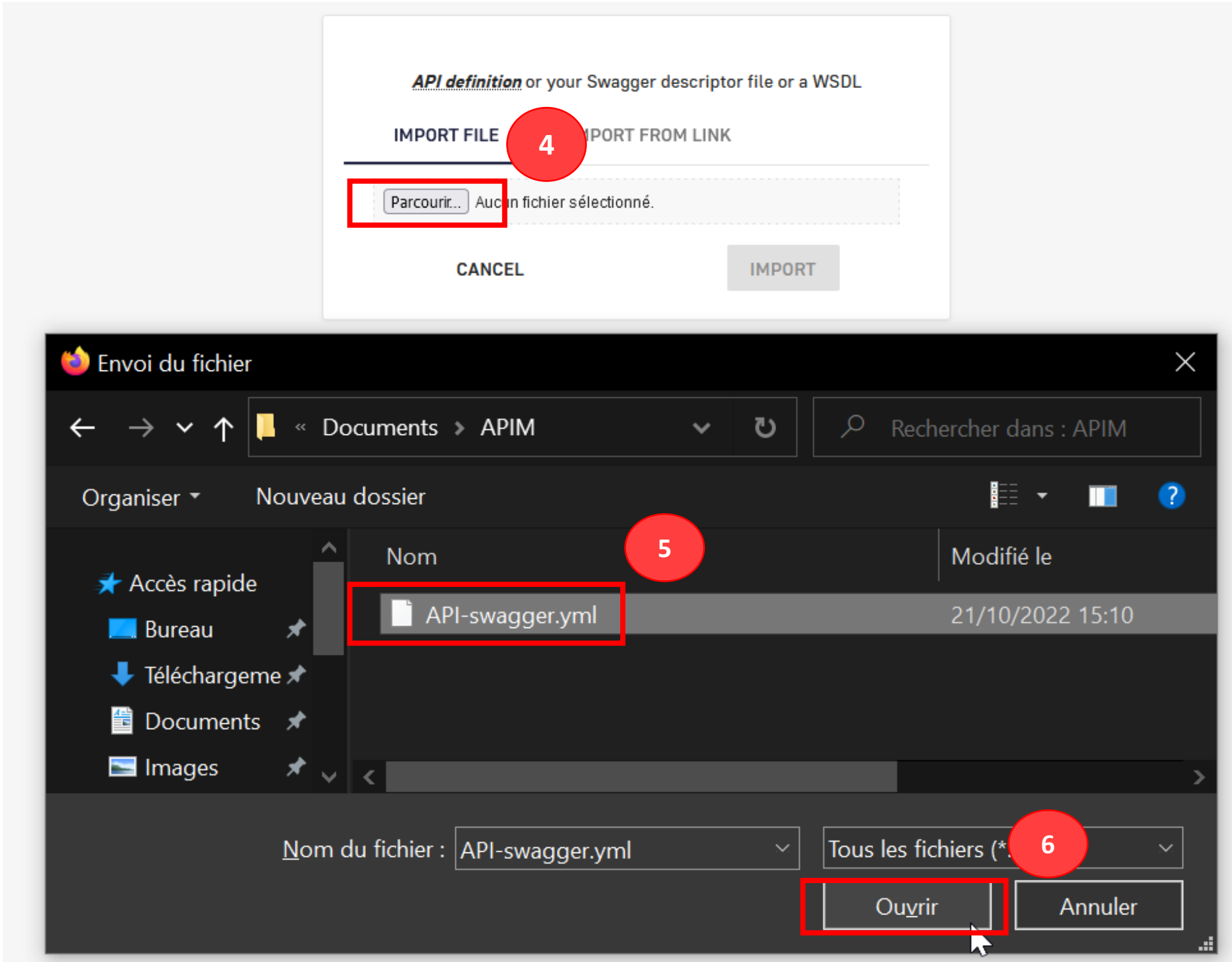
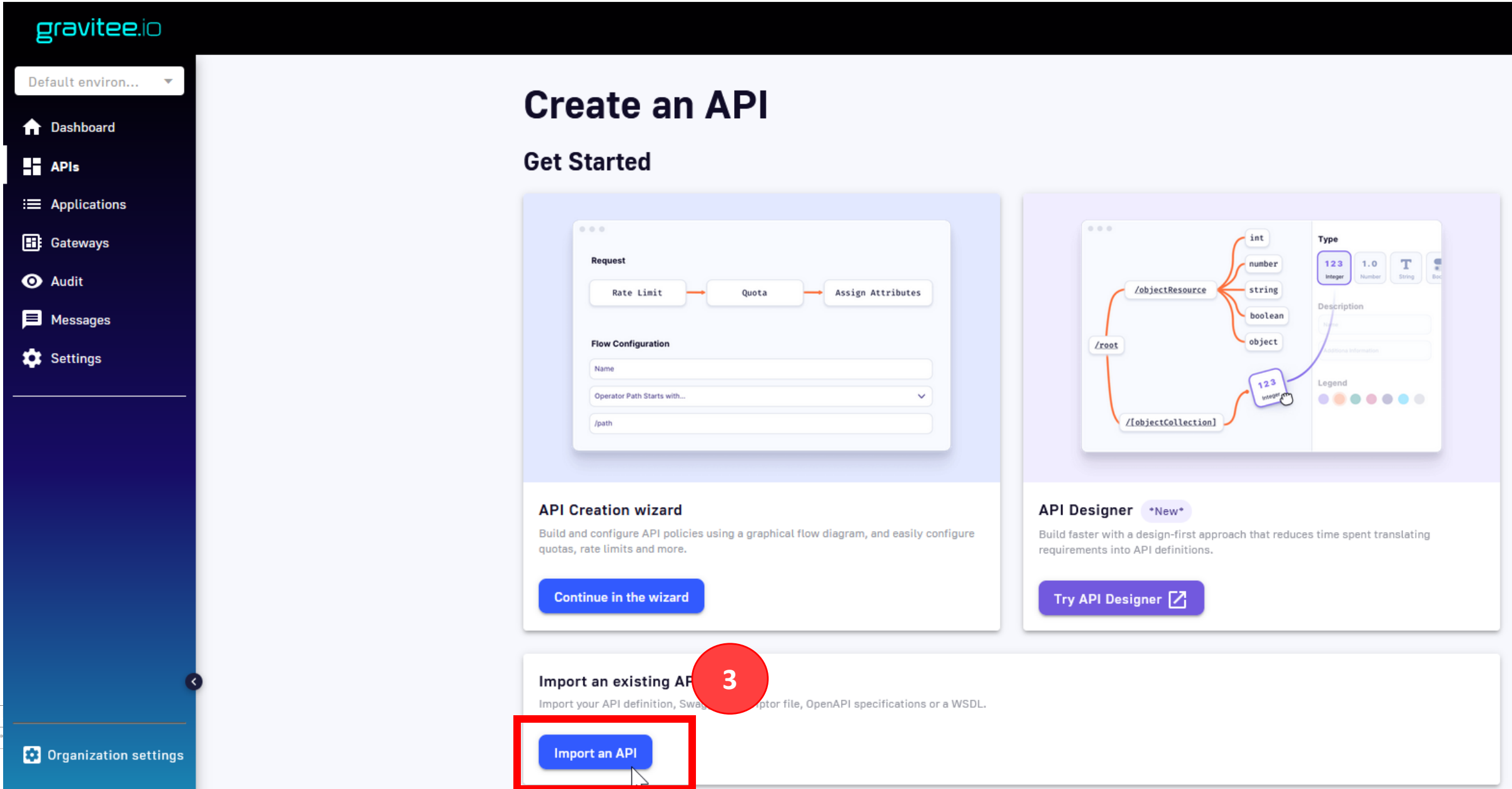
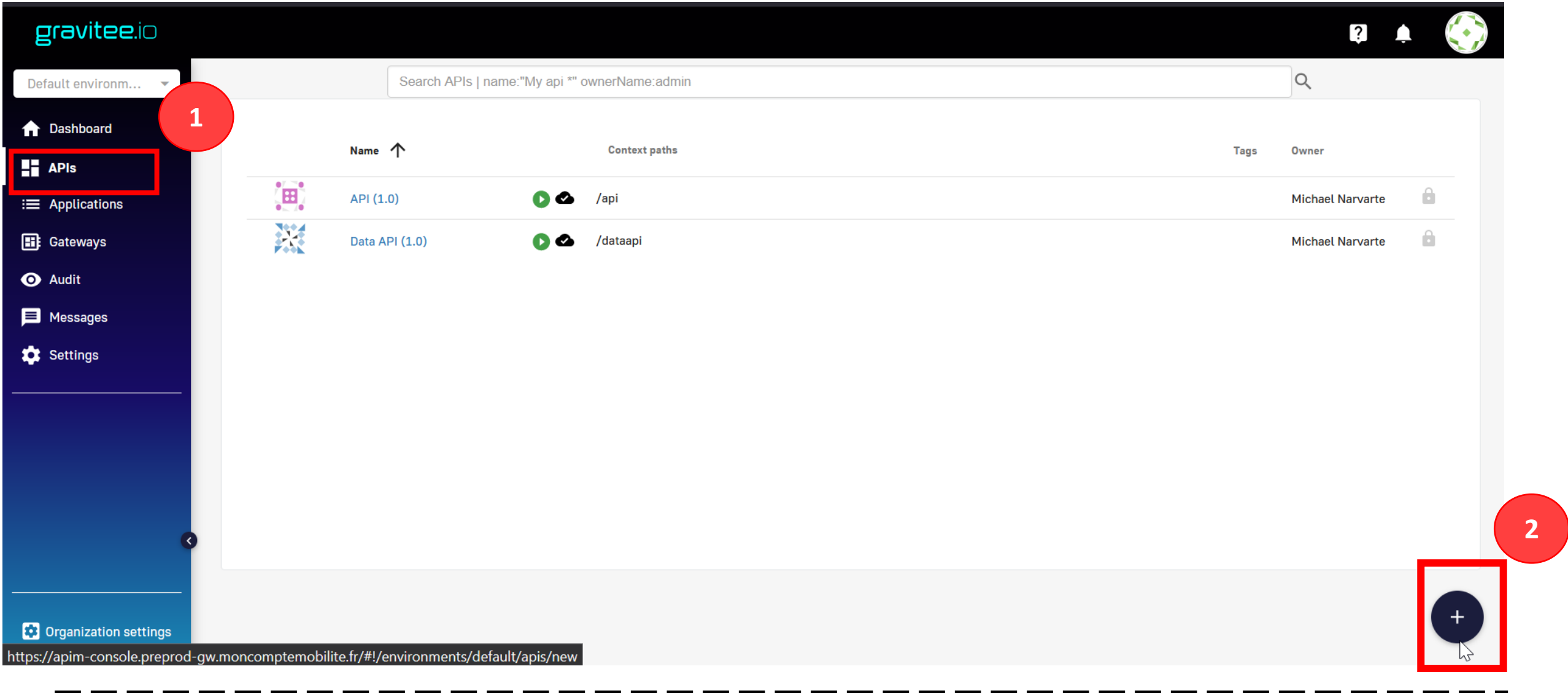
- Avoir un **compte administrateur Gateway**
- Accéder à l'URL de l'APIM console selon l'environnement :  
  
`https://apim-console.[env]-[domain]/#!/environments/default/`
- Récupérer les swaggers des API que l'on souhaite configurer :
  - API
  - Data-API
- S'assurer que la version dans le swagger correspond à la version actuelle des API et que les URLs serveurs correspondent à celle de l'environnement

## 2. Créer une API



# Création d'une API – Option 1

## Créer une nouvelle API from scratch



# Création d'une API – Option 1

## Créer une nouvelle API from scratch

**API definition** or your Swagger descriptor file or a WSDL

IMPORT FILE    IMPORT FROM LINK

Parcourir... API-swagger.yml

**Swagger import configurations:**

- ☒ **Create documentation**  
Add a documentation page with the content of the swagger descriptor.
- ☒ **Create the path-mapping for analytics**  
Create each path from the swagger descriptor.
- ☐ **Create policies on paths**  
Create each path from the swagger descriptor.
  - ☐ Apply JSON Validation policy  
Apply policy on each path from the swagger descriptor.
  - ☐ Apply Mock policy  
Apply policy on each path from the swagger descriptor.
  - ☐ Apply Rest to SOAP Transformer policy  
Apply policy on each path from the swagger descriptor.
  - ☐ Apply Validate Request policy  
Apply policy on each path from the swagger descriptor.
  - ☐ Apply XML Validation policy  
Apply policy on each path from the swagger descriptor.

CANCEL    **IMPORT**

gravitee.io

Default environm...

Test API (1.0)

**General**

Name \* Test API    Version \* 1.0

Description \* Swagger for the Gateway API

Owner Amal GHADAB    Created at a few seconds ago    Last deployment at

Labels Enter a label

Portal categories

SAVE    RESET    EXPORT    IMPORT    DUPLICATE    PROMOTE

**Danger Zone**

Start the API. It will be available on all gateways (depending on sharding tags).

Publish the API. It will be available on portal (depending on visibility/rights).

Make this API public. Everyone can see it.

Deprecate this API. It will no longer be published on portal.

**API out of sync, deploy your API**

**START THE API**

**PUBLISH THE API**

MAKE PUBLIC

DEPRECATE

Would you like to deploy your API?

You can provide a label to identify your deployment

Deployment label

CANCEL    **OK**

Are you sure you want to start the API?

CANCEL    **START**

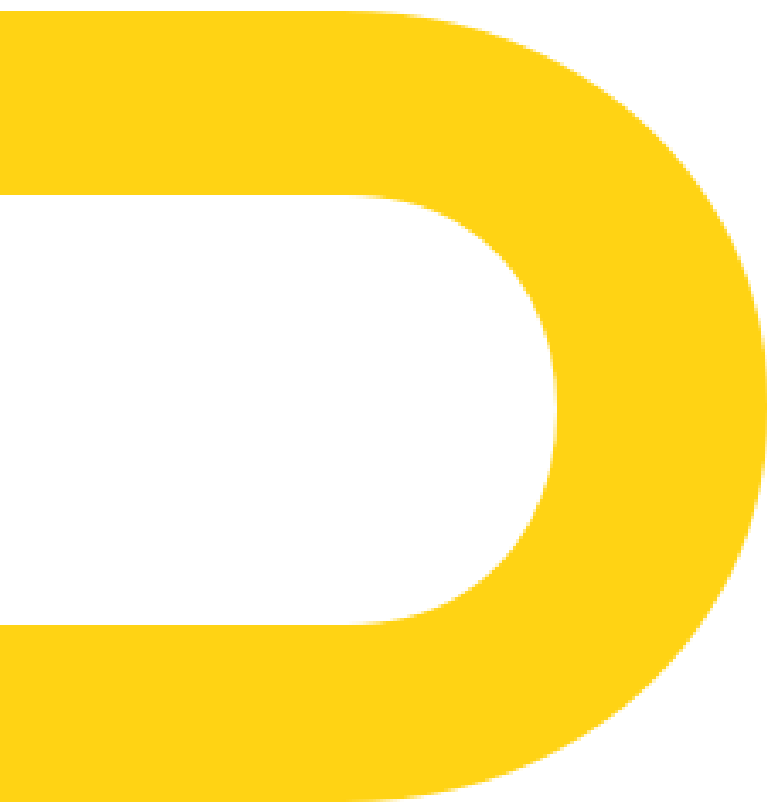
7

Une fois l'API créée, il est nécessaire de faire un **'deploy'** après chaque modification de l'API pour la mettre à jour.

- Le déploiement se fait en interne au niveau de l'API Gravitee
- A cette étape (**étape 7**) de la configuration :

9

- l'API n'est pas encore visible par la Gateway Gravitee, pour la rendre visible faudra cliquer sur le bouton **'Start the API'** (**étape 9**)
- l'API n'est pas encore visible par le portail Gravitee, une fois la configuration de l'API finalisé, faudra la publier en cliquant sur le bouton **'Publish the API'** (**étape 11**). Cette action est à faire à la fin de la configuration



# Création d'une API depuis une configuration existante





# Création d'une API – Option 2

## Exporter une configuration existante depuis un autre environnement

- Il est possible d'**exporter une API existante** d'un environnement à un autre.
- L'exportation d'une API existante permet d'exporter toutes sa configuration (groups, membres, pages, plans, policies, ...)
  - Un fichier .Json sera créer lorsqu'on clique sur le bouton **Export**

gravitee.io

Default environm...

Dashboard

**APIs**

Applications


Gateways


Audit

Search APIs | name:"My api \*" ownerName:admin

Name ↑

Context paths

 API (1.0) /api

 Data API (1.0) /dataapi

Default environm...

API (1.0)

Details

GENERAL

Details

PLANS

Plans

Subscriptions

DOCUMENTATION

Pages

Metadata

USER AND GROUP ACCESS

Members

Groups

Transfer ownership

General

Name \*

API

Version \*

1.0

Description \*

Swagger for the Gateway API

Owner

Michael Navarte

Created at

Sep 15, 2022

Last deployment

2 days ago

Labels

Enter a label

Portal categories

SAVE

RESET

**EXPORT**

IMPORT

DUPLICATE

PROMOTE

Export API definition as :

Current version (3.18.11)

What do you want to export ?

☒ Groups

☒ Members

☒ Pages

☒ Plans

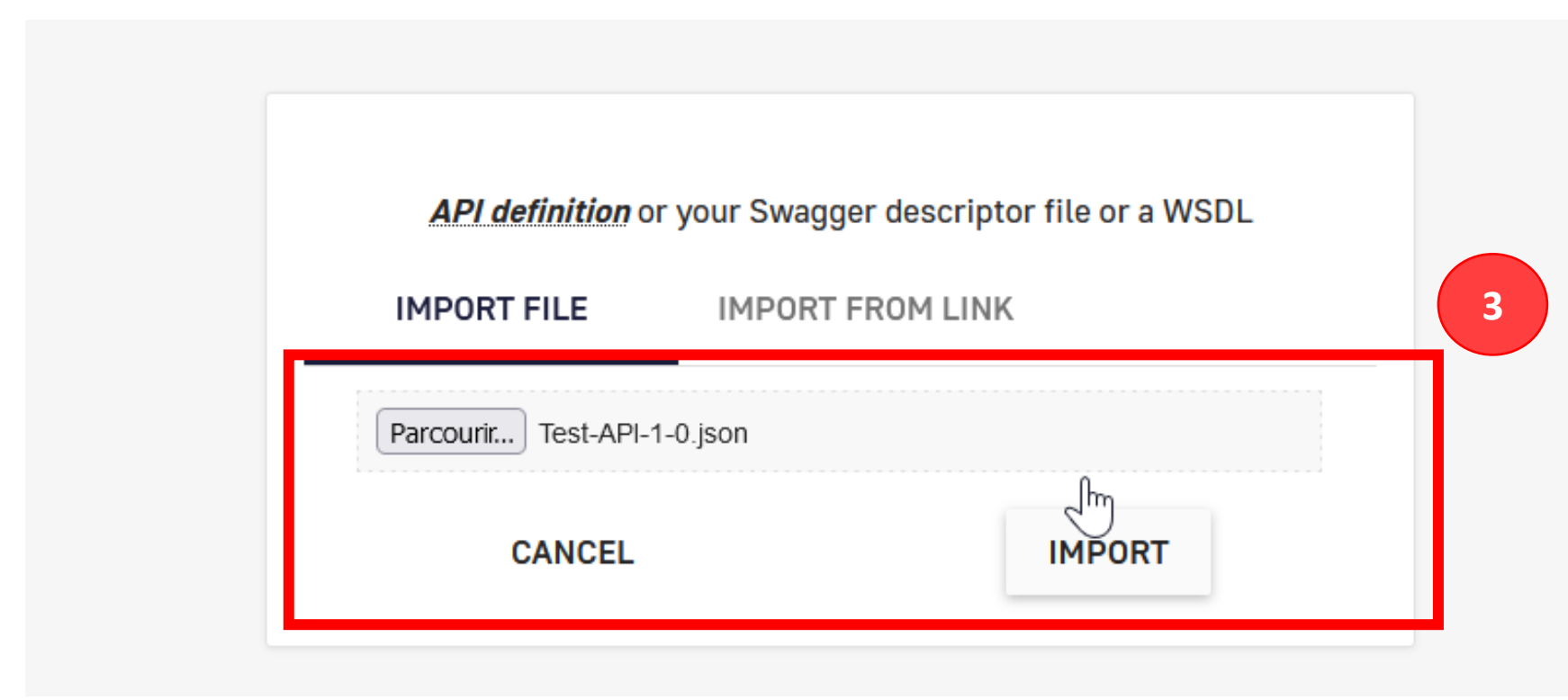
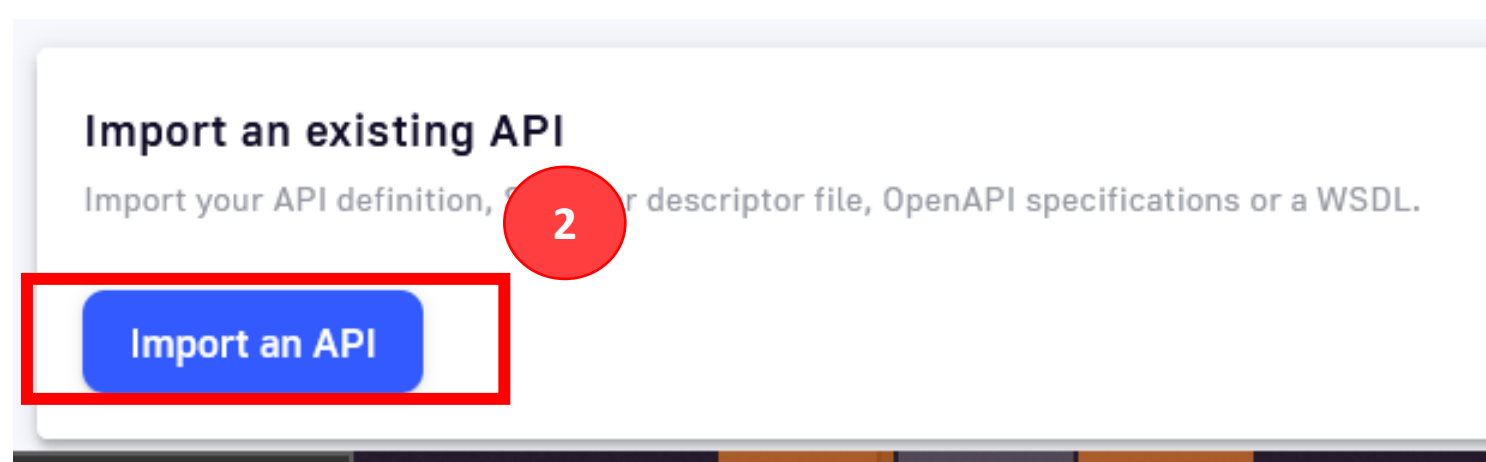
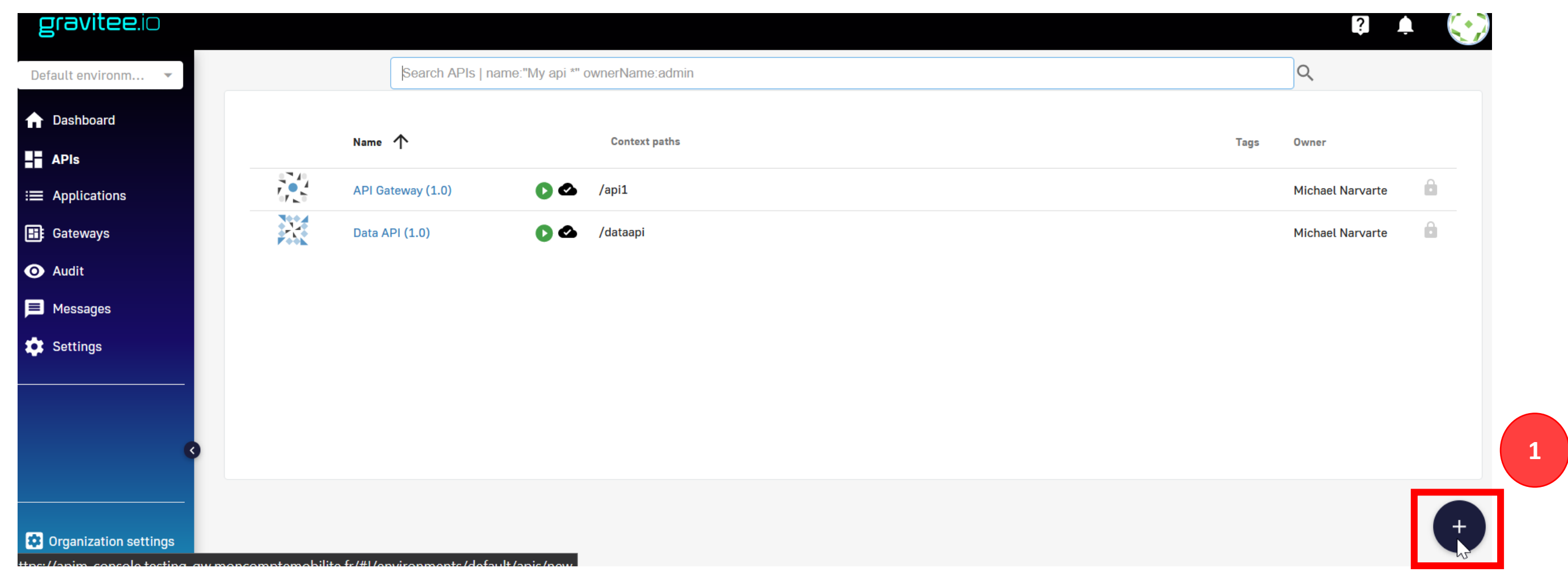
☒ Metadata

CANCEL

**EXPORT**

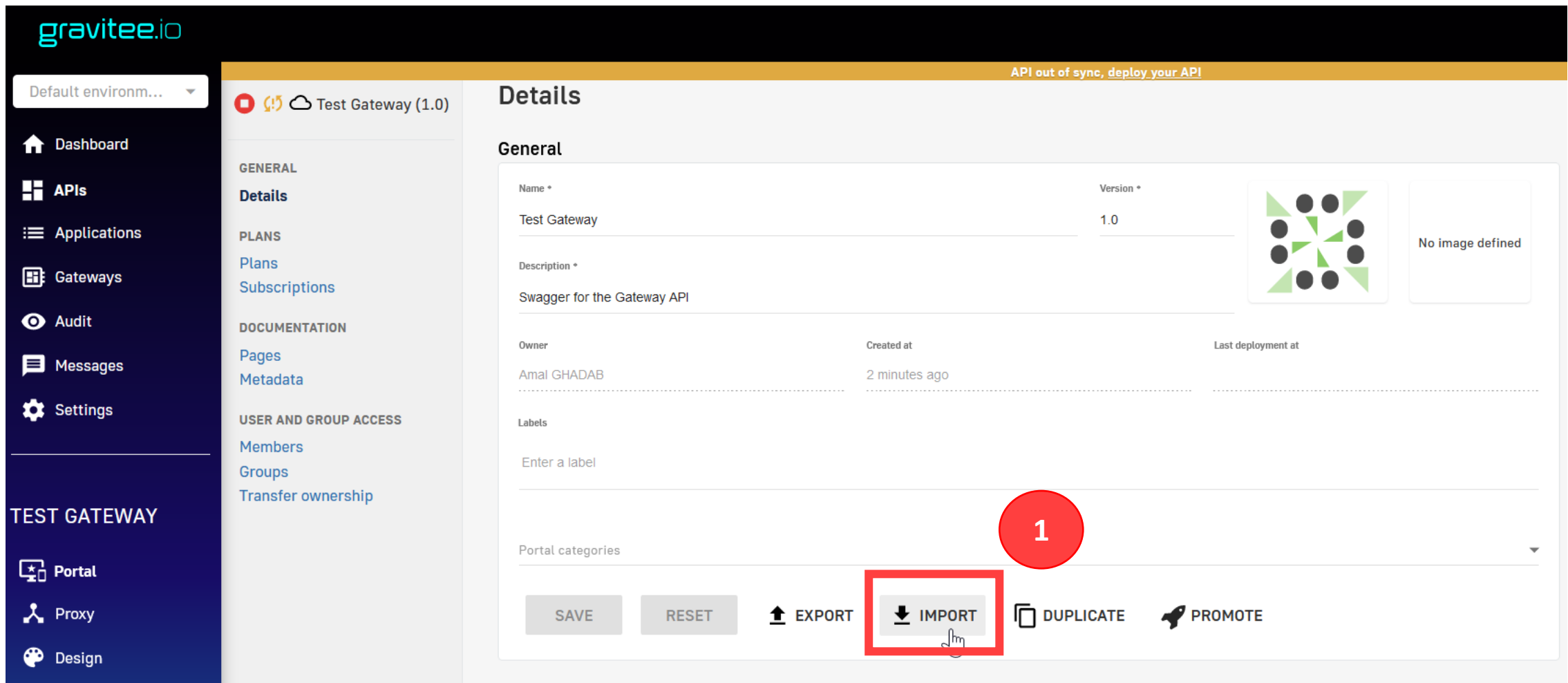
# Création d'une API – Option 2

## Importer une API depuis un autre environnement



# Création d'une API – Option 2

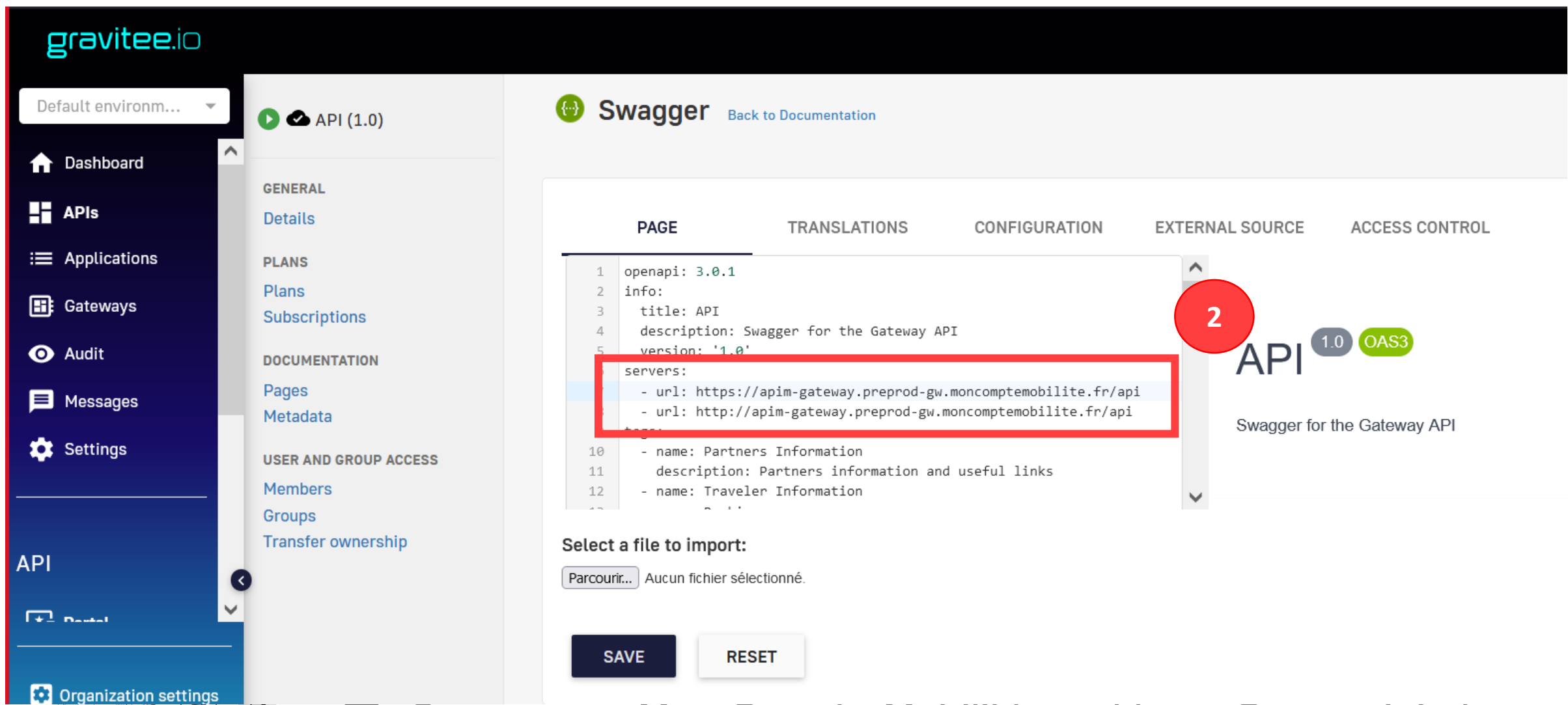
## Importer une configuration d'une API



### Prérequis à vérifier

Il est également possible **d'importer les configurations d'une API existante** depuis un environnement 1 pour configurer la même API sur autre environnement 2.

- 1 Dans l'onglet détails, il faudra cliquer sur le bouton **Import** pour sélectionner le json exporter auparavant
- 2 Une fois l'import effectué, vérifier les **plans**, le **context-path** et l'**url backend** dans le menu **proxy** ainsi que les URLs dans le swagger accessible depuis le menu **Pages**







## 3. Créer des plans

# Création des plans

Un plan fournit un service et une couche d'accès à une API. Le plan spécifie les limites d'accès ainsi que le mode de souscription à un API pour un partenaire donné afin de répondre à des besoins spécifiques. Des règles sont appliquées par la suite sur des plans pour autoriser ou refuser l'accès aux certains / à l'ensemble des endpoints de l'API

gravitee.io

Default environm...

Test API (1.0)

Dashboard

APIs

Applications

Gateways

Audit

Messages

Settings

TEST API

Portal

Proxy

GENERAL

Details

PLANS

Plans

Subscriptions

DOCUMENTATION

Pages

Metadata

USER AND GROUP ACCESS

Members

Groups

Transfer ownership

General

Name \*

Test API

Version \*

1.0

Description \*

Swagger for the Gateway API

Owner

Amal GHADAB

Created at

a few seconds ago

Last deploym

a few sec

Labels

Enter a label

Portal categories

SAVE

RESET

EXPORT

IMPORT

DUPLICATE

PROMOTE

Test API (1.0)

GENERAL

Details

PLANS

Plans

Subscriptions

DOCUMENTATION

Pages

Metadata

USER AND GROUP ACCESS

Members

Groups

Transfer ownership

Plan

1 Define

2 Secure

3 Restrictions

General

Name \*

MaaS1\_partner\_plan

Plan name

18 / 50

Description \*

Plan pour application MaaS 1

Provide a description of your plan, what it does, ...

Characteristics

Preview

MaaS1\_partner\_plan

Authentication:

Plan pour application MaaS 1

Plans

Staging

Published

Deprecated

Closed

Plans will appear here

Start creating a plan

+

3

Renseigner le nom et la description du plan, puis cliquer sur le bouton **Next**

# Création des plans

Test API (1.0)

GENERAL

Details

PLANS

Plans

Subscriptions

DOCUMENTATION

Pages

Metadata

USER AND GROUP ACCESS

Members

Groups

Transfer ownership

Plan

Define

Secure

Restrictions

Authentication

Authentication type \*

API Key

Select the type of authentication

Configuration

Propagate API Key to upstream API

Additional selection rule

Selection Rule

Define an additional rule when you're managing multiple plans of the same type to improve the plan's selection process. For example, if you want to check the issuer of a jwt token: `#context.attributes['jwt'].claims['iss'] == 'my-issuer'`

PREVIOUS

CANCEL

NEXT

Test API (1.0)

GENERAL

Details

PLANS

Plans

Subscriptions

DOCUMENTATION

Pages

Metadata

USER AND GROUP ACCESS

Members

Groups

Transfer ownership

Plan

Define

Secure

Restrictions

Rate Limiting

Rate limit how many HTTP requests an application can make in a given period of seconds or minutes

Quota

Rate limit how many HTTP requests an application can make in a given period of hours, days or months

Resource Filtering

Restrict resources according to whitelist and / or blacklist rules

PREVIOUS

CANCEL

SAVE

- 4

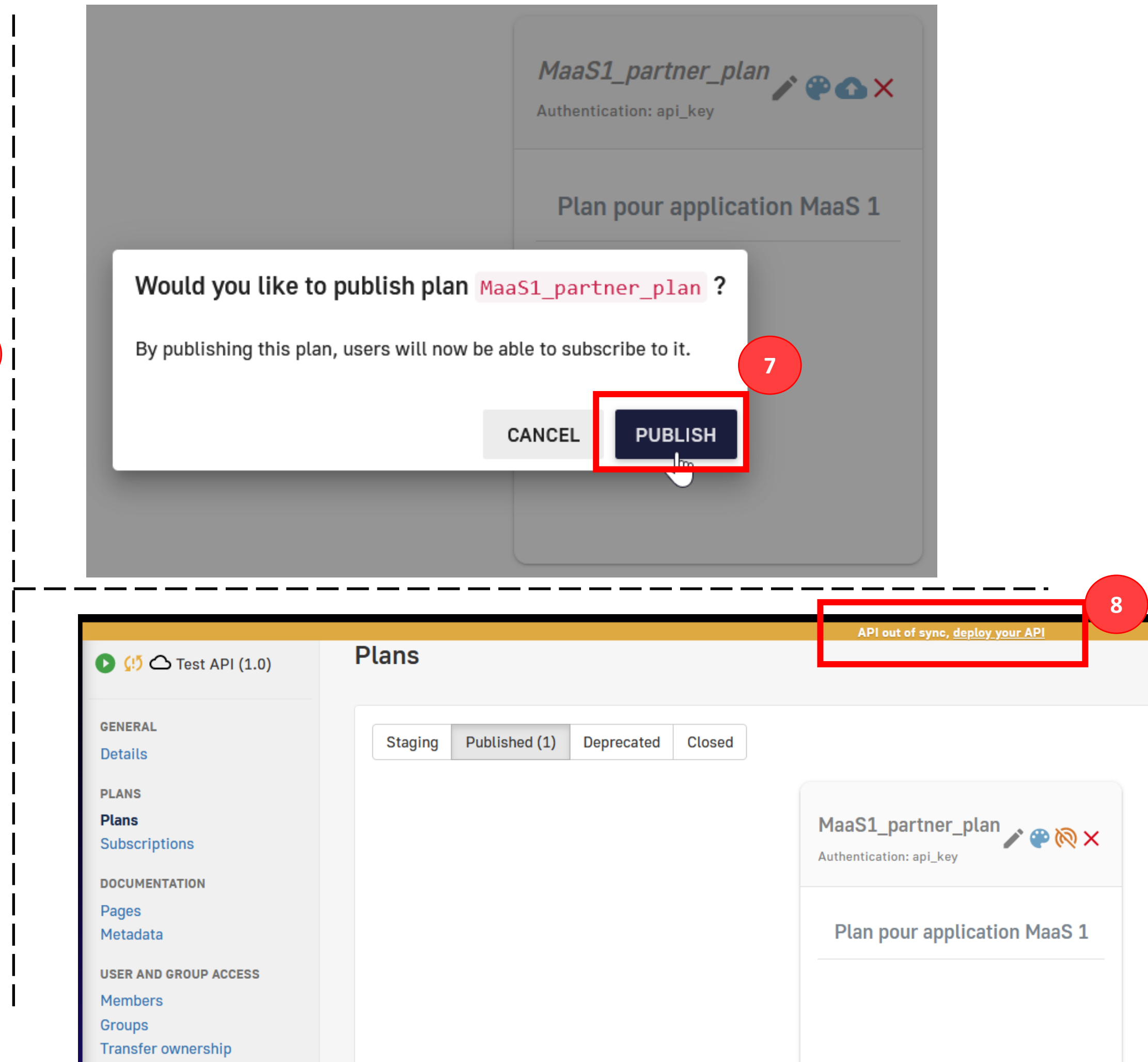
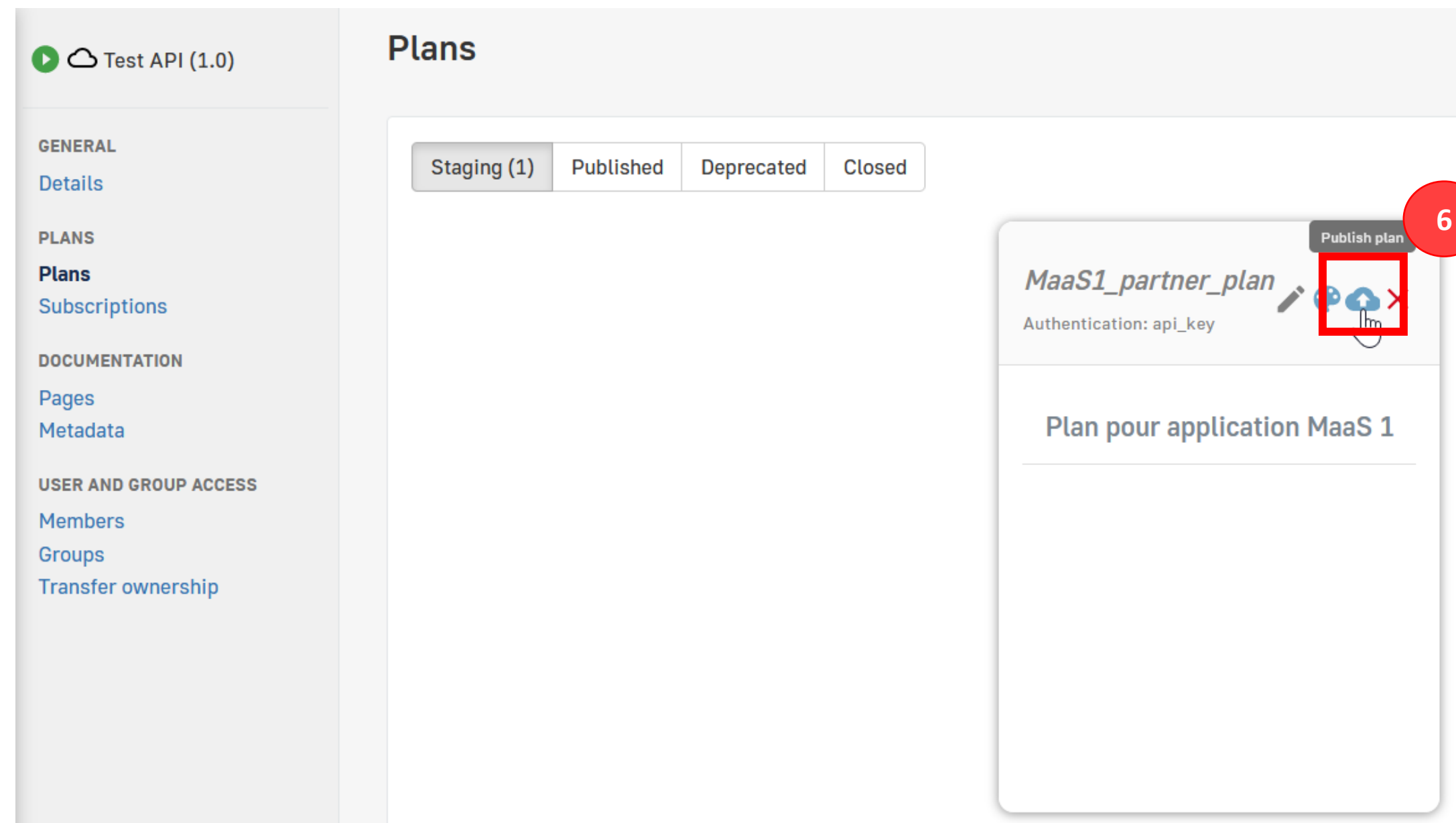
Saisir le champ **Authentication type**, en sélectionnant dans la liste "security type" la valeur **API Key**
- Puis, cliquer sur **Next**
- 5

A l'étape suivante, on ne coche aucune case, on clique directement sur **Save** pour sauvegarder le plan



# Création des plans

## Publier un Plan



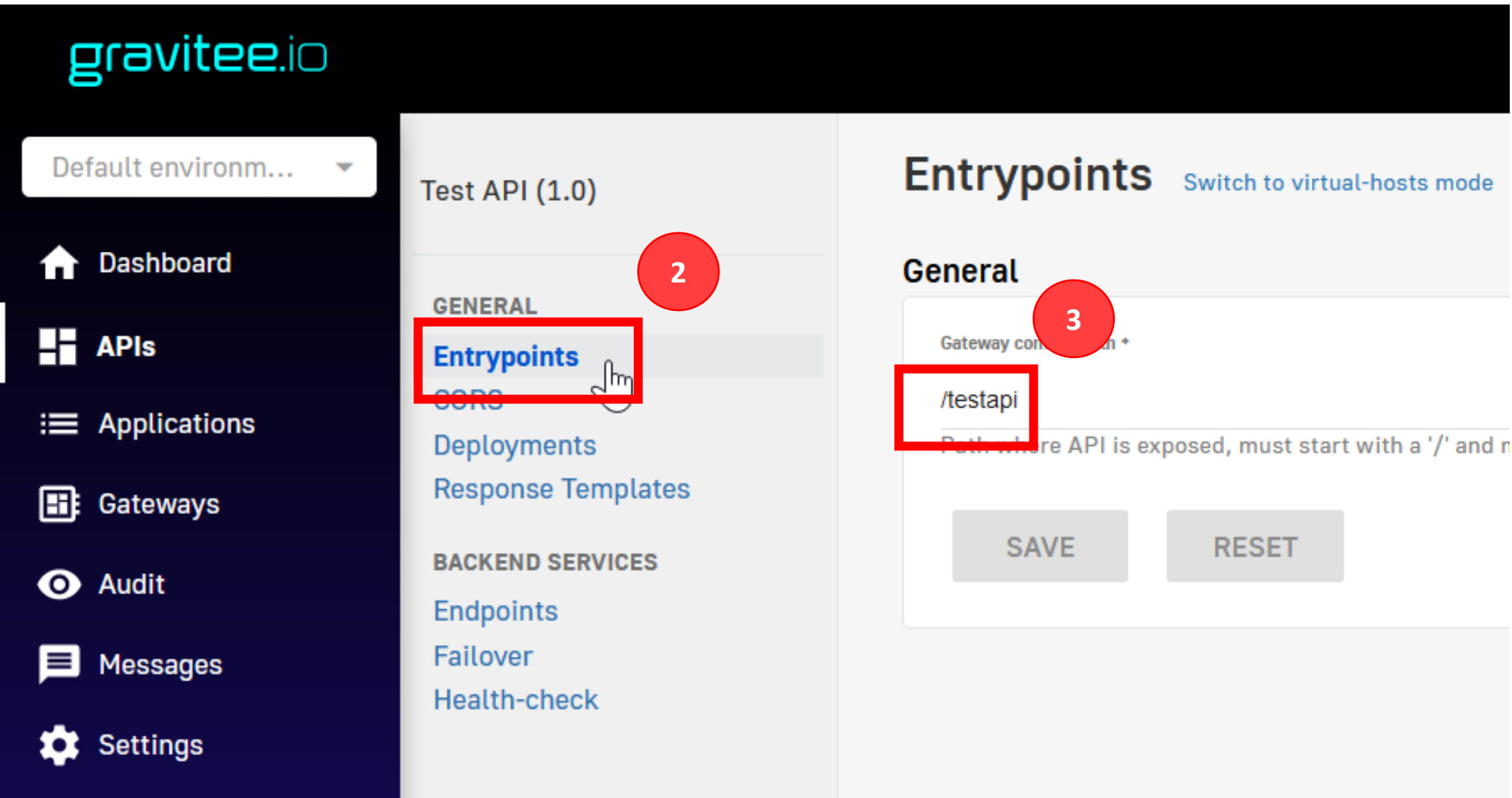
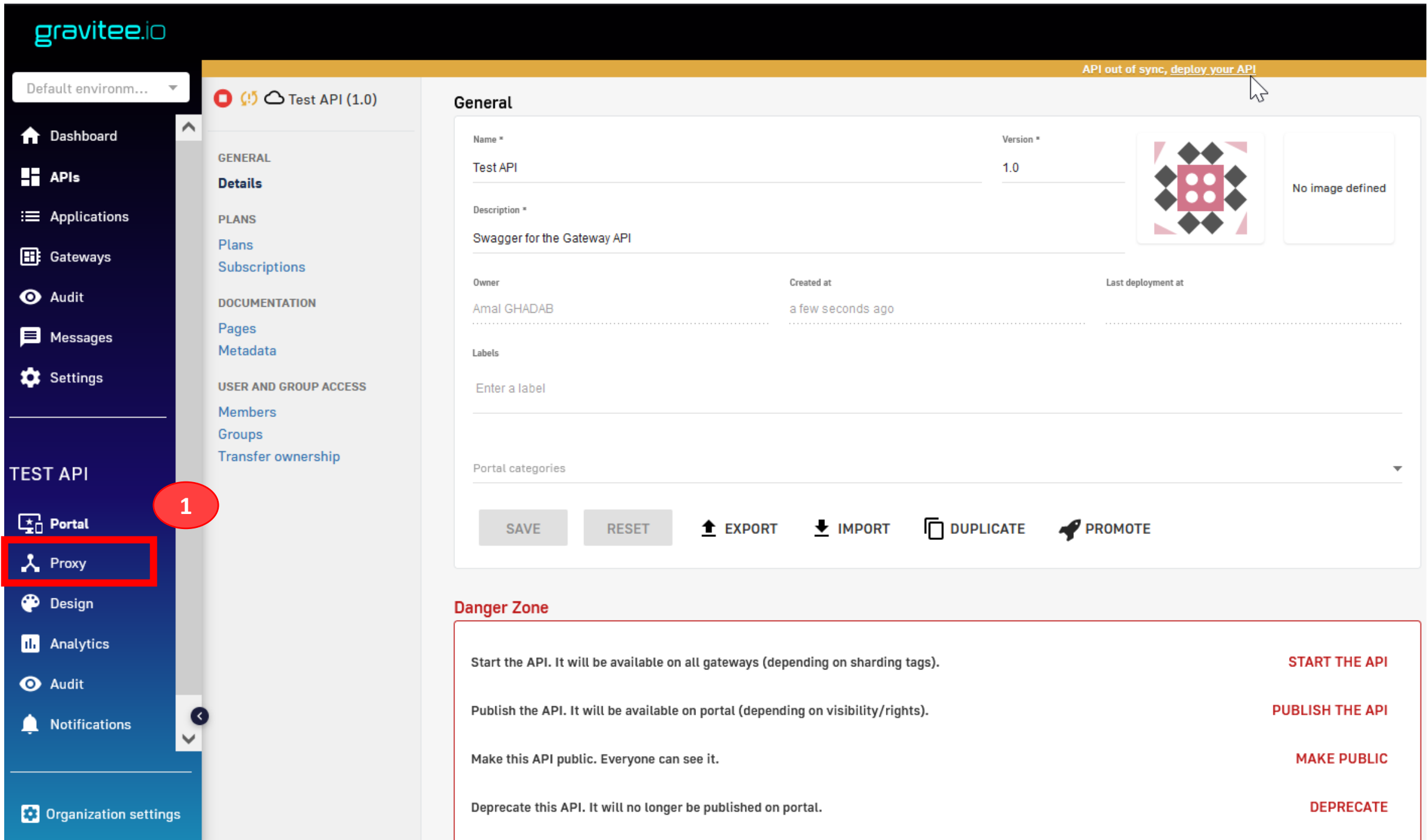
6 Publier le plan afin qu'il soit visible et utilisable par les applications partenaires.

8 Ne pas oublier de faire un nouveau **deploy** pour enregistrer les modifications

# 4.Configuration des APIs

# Configuration des API

## Configurer l'URL d'accès à l'API



3

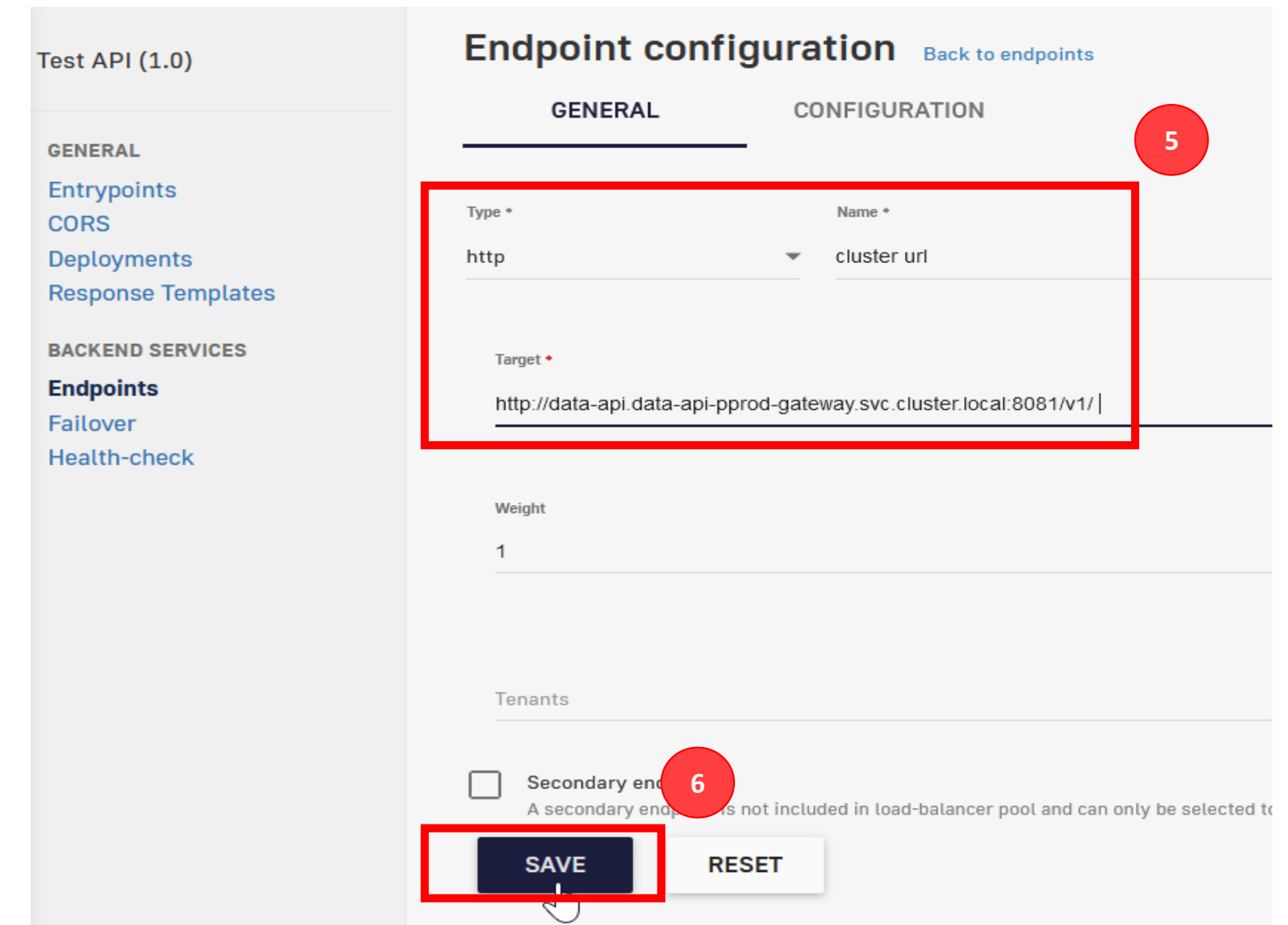
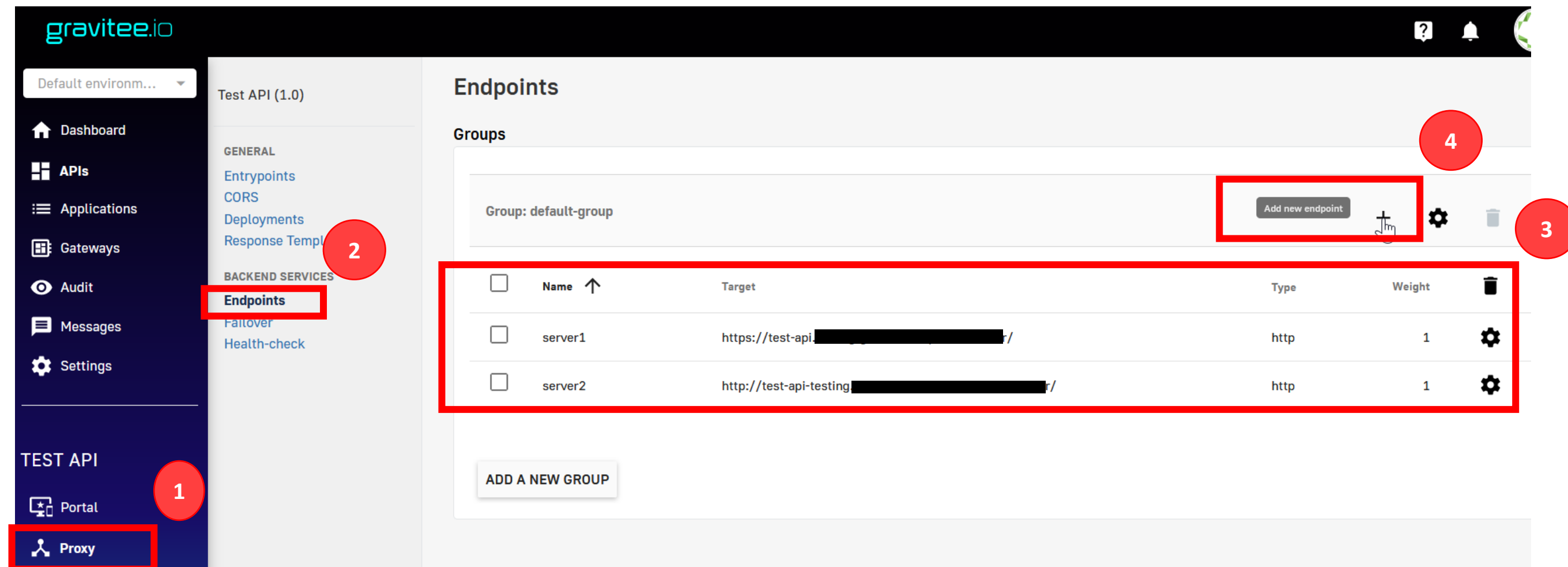
Dans l'input **Gateway context-path**, vérifier que l'url saisie correspond bien à ce que l'on souhaite utiliser lorsqu'on appellera les api

Cette URL permettra d'accéder aux endpoints de l'API en saisissant l'URL de l'APIM Gateway suivi de ce context-path (ex: [https://apim-gateway.\[env\].\[domain\]/testapi](https://apim-gateway.[env].[domain]/testapi) )



# Configuration des API

## Configurer les URLs d'accès au backend de l'API



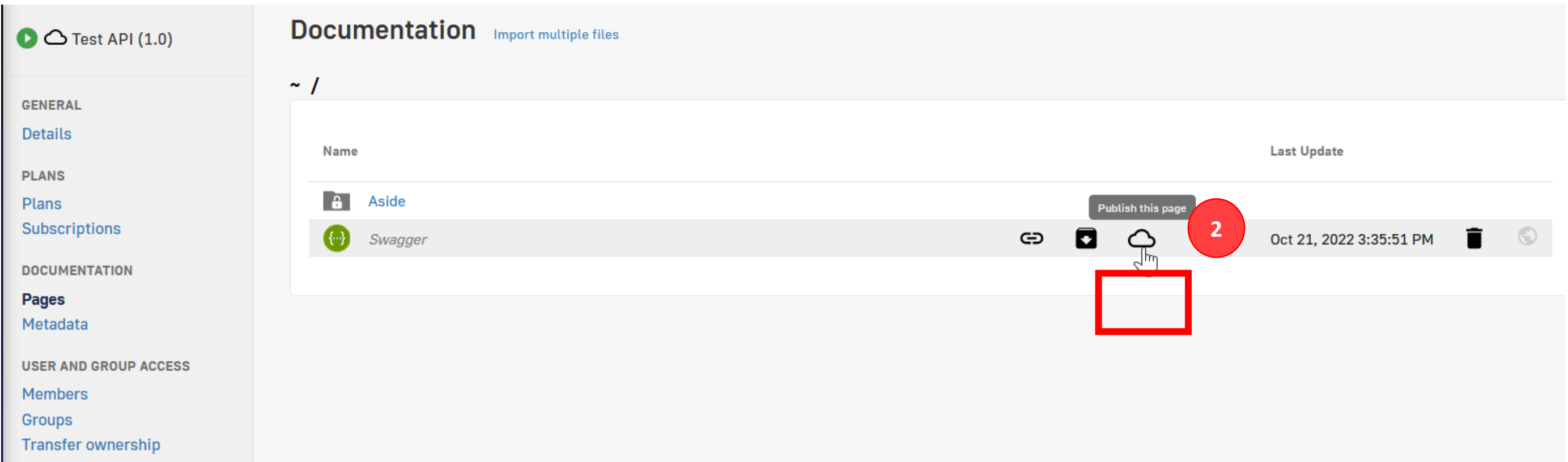
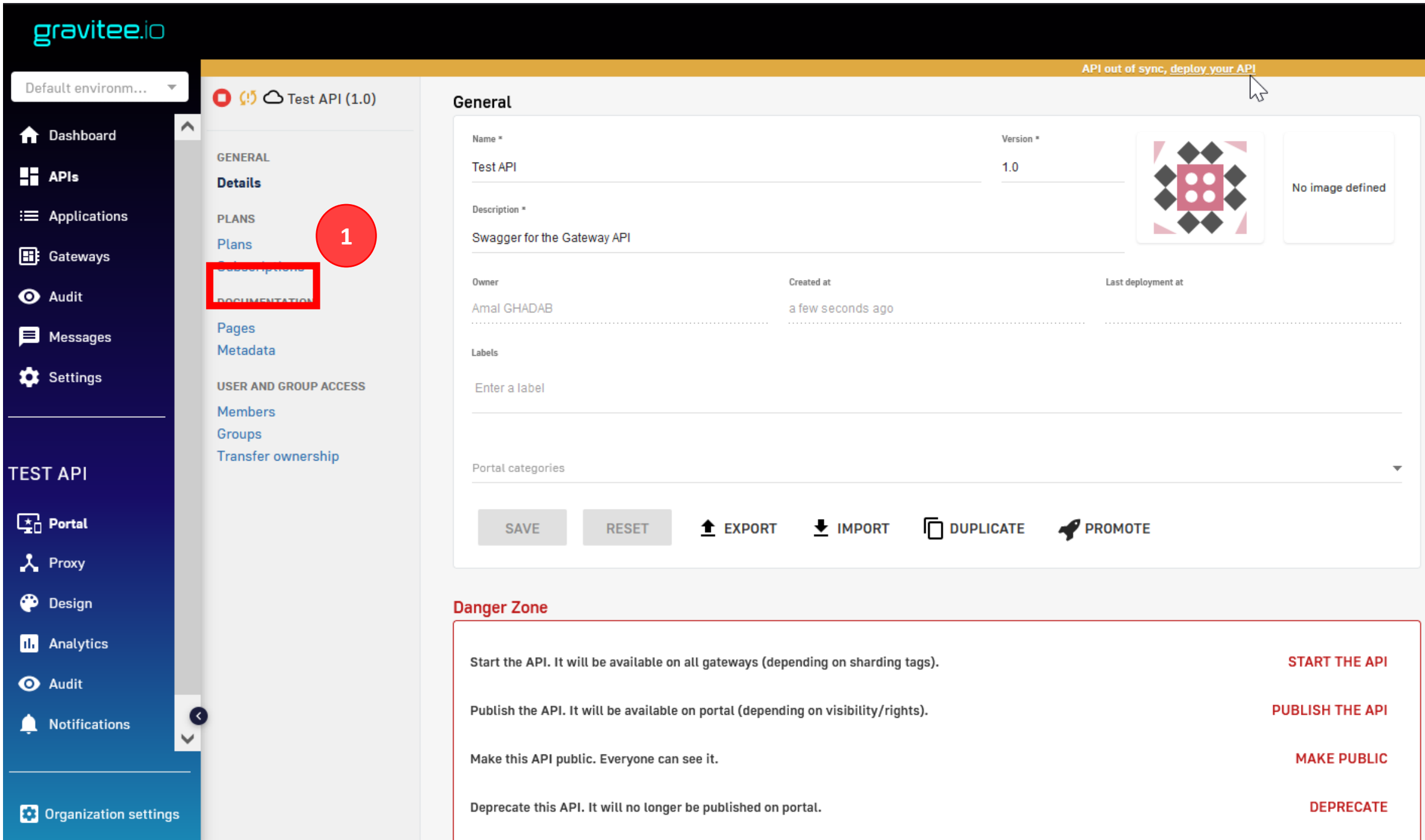
- 3 Dans la section **Endpoints**, vérifier les URLs générées par défaut en se basant sur le swagger correspondent bien aux URLs du backend permettant d'appeler l'API
- Les URLs doivent être au format interne **SVC** (ex. <http://test-api.test-api-pprod-gateway.svc.cluster.local:8081/v1/>)
  - Si dans la liste générée par défaut, les URLs ne sont pas bonnes, il faudra les supprimer en cochant ces URLs erronées, puis, en cliquant sur l'icone supprimer
- 4 Pour rajouter une nouvelle URL, cliquer sur l'icone **+** :
- Renseigner les champs **type** (http), le **nom** de l'url du serveur et le **target** (l'URL svc du microservice backend appelé par l'API)
  - Une fois les champs renseignés, on clique sur **save** pour sauvegarder l'URL

Ne pas oublier de faire un nouveau **deploy** pour enregistrer les modifications

# **5. Publication de la documentation d'une API**

# Publication de la documentation d'API

## Rendre le swagger d'une API visible au niveau portail



2 Une fois la publication du swagger activée, celui-ci sera visible au niveau du portail. Les partenaires peuvent alors visualiser les différents endpoints exposés par cette API avant de souscrire à cette dernière, en fonction des plans qui leurs seraient proposées et qui correspondraient à leur besoin.



## **6. Définition des policies sur les plans d'API & endpoints**

# Définition des politiques sur les plans d'API et / ou les endpoints

## Rendre le swagger d'une API visible au niveau portail

The first screenshot shows the Gravitee.io dashboard with the 'Design' menu highlighted (1). The 'Plans' section is visible, showing three plans: MaaS\_Partners, MSP\_Partners, and Admin. The 'Design plan' icon is highlighted (2).


The second screenshot shows the 'Design' view for the 'MSP\_Partners' plan. The 'Resource Filtering' policy is highlighted (3). The 'Security' menu is highlighted (4). The 'Resource Filtering' policy is selected (5). The 'Whitelist' rules are shown (6). The 'Save' button is highlighted (7).

Pour configurer les politiques il est possible d'accéder à la page de 2 façons:

1. Depuis le menu Design
2. Depuis les plans en cliquant **sur l'icone** 

Il est possible d'appliquer des règles soit sur des plans (déjà créés), soit sur des endpoints spécifiques (dans ce cas là, les règles sur ces endpoints vont être appliquées sur tous les plans)

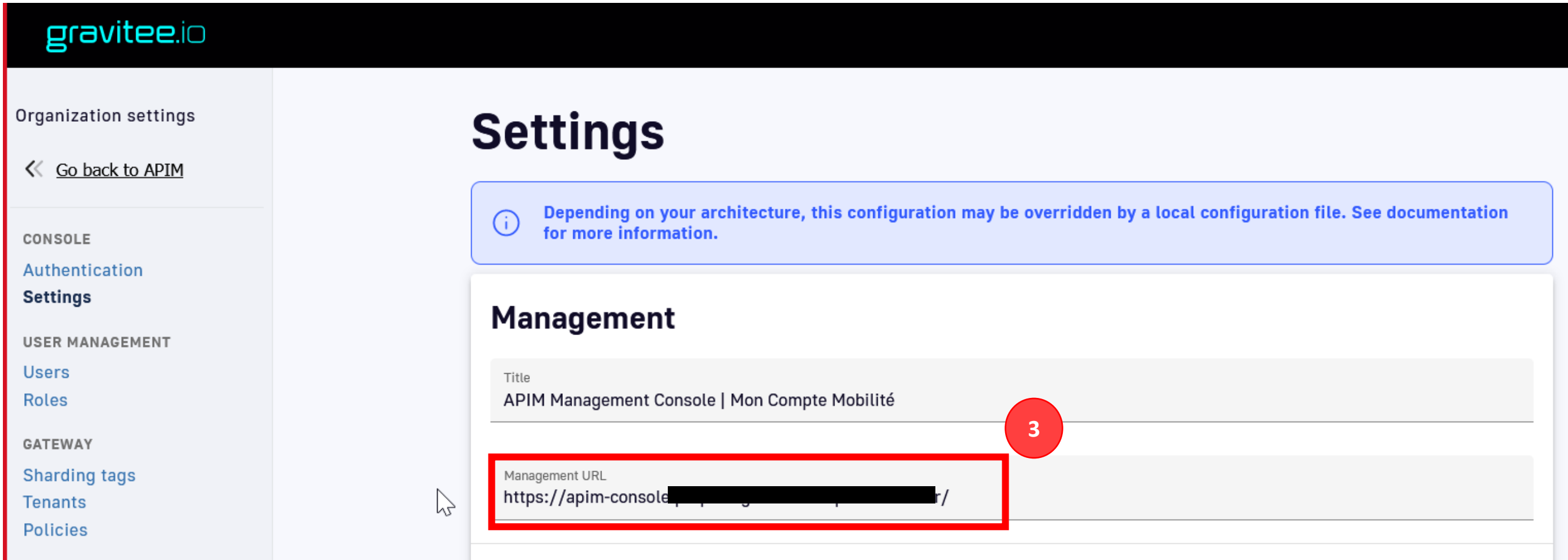
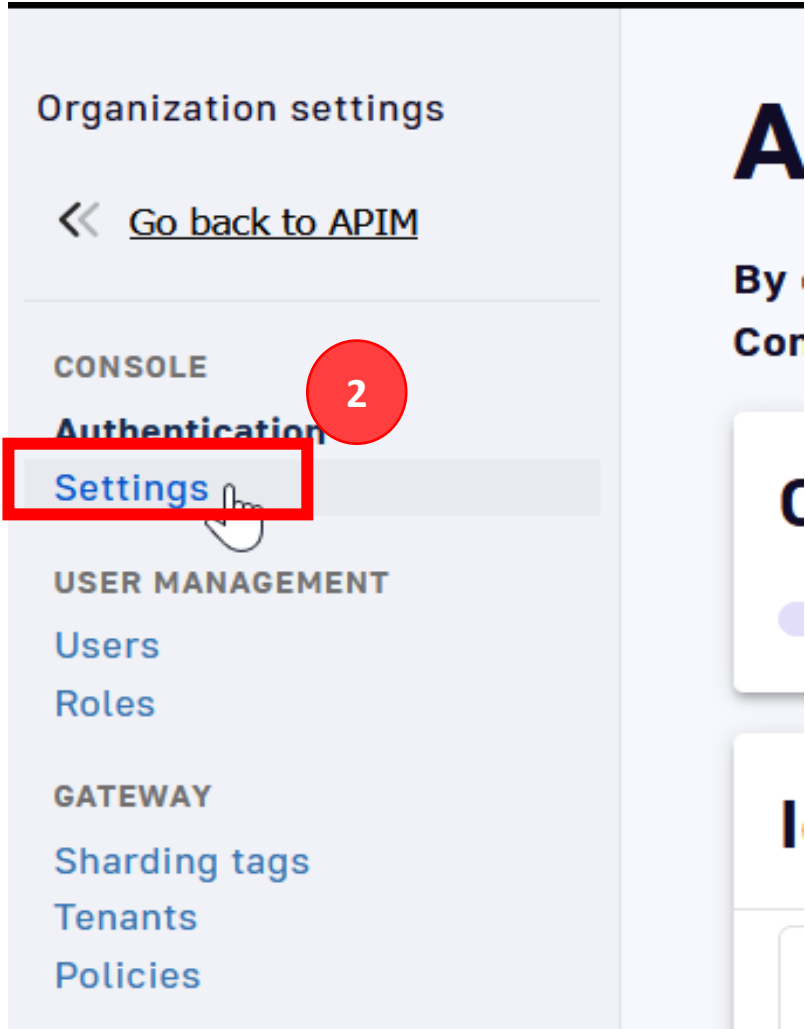
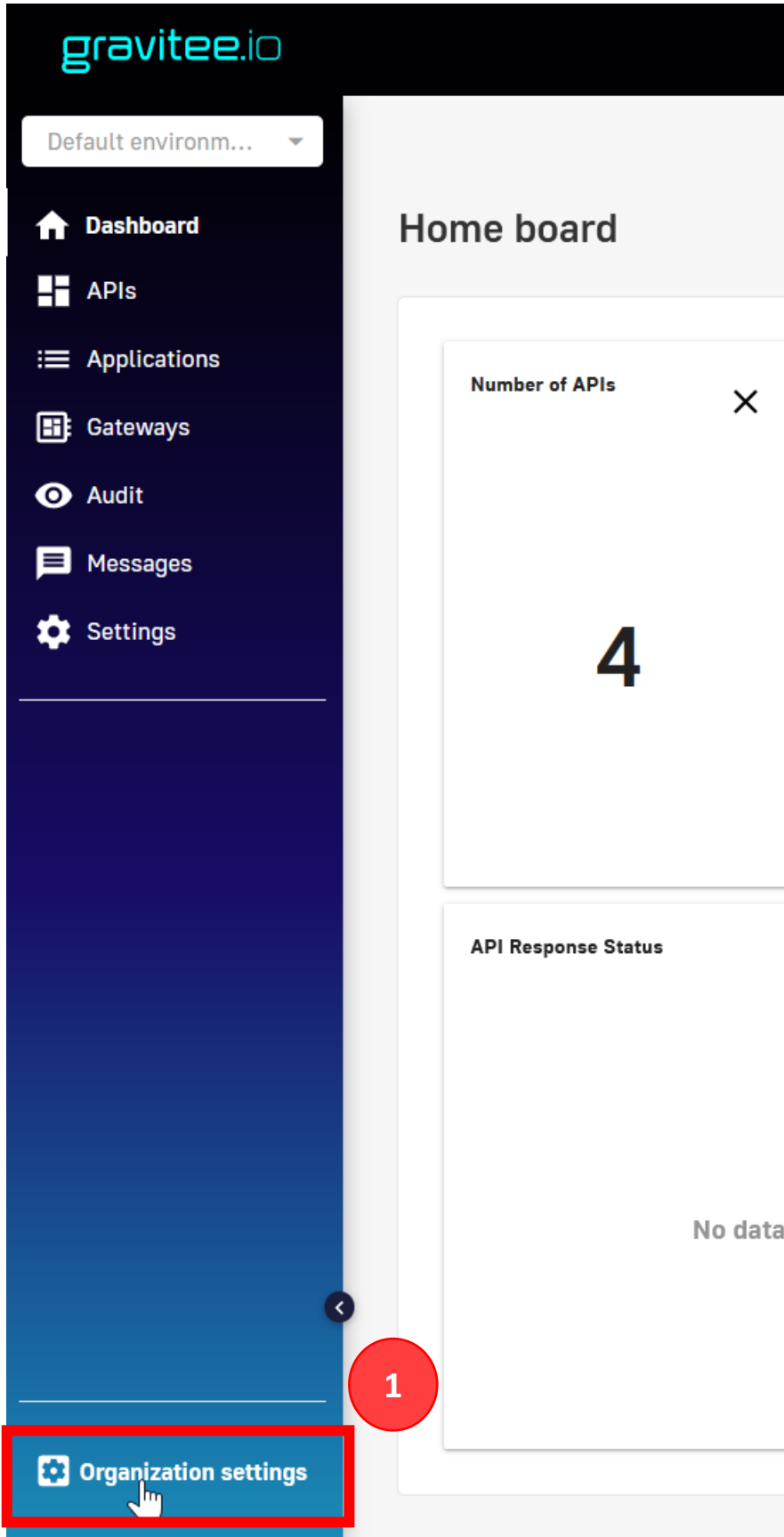
Pour appliquer une policy sur un plan:

3. Sélectionner le **plan**
4. Dans le menu **security** à droite, choisir la policy à utiliser en la glissant dans le cadre request et/ou réponse en fonction du besoin (ex: **Resource filtering** dans request pour filtrer les appels entrants).
5. Cliquer sur la policy pour pouvoir la configurer
6. Configurer les URLs autorisés ou à rajouter dans la blacklist en spécifiant la méthode.
7. Une fois la config terminée, cliquer sur l'icone  pour valider cette conf, puis sur le bouton **save** pour enregistrer les modification et à la fin, ne pas oublier de faire un **deploy**
- Un plan peut avoir plusieurs politiques

# 7. Autres configurations

# Autres configurations

## Modification du Management URL



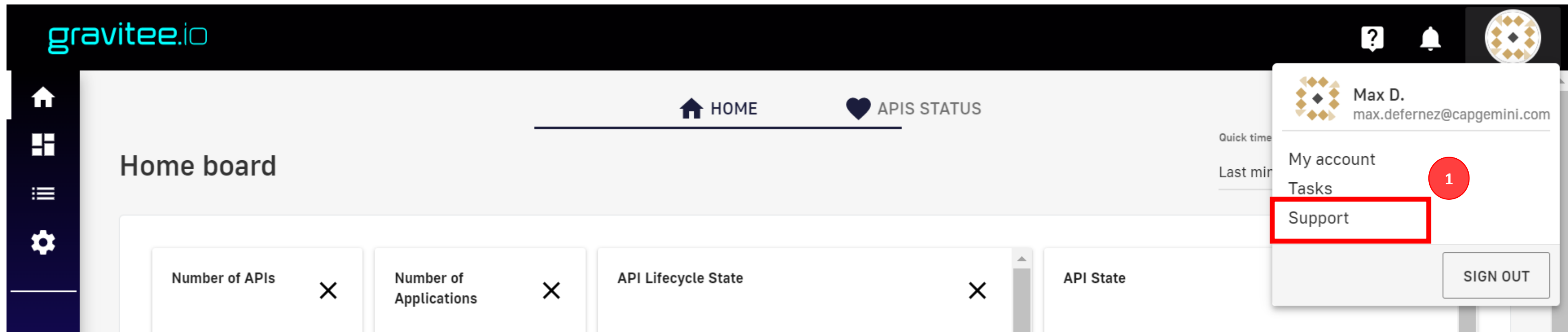
3 Modifier l'URL du champ Management URL en saisissant l'url de l'APIM console



# 7. Tickets

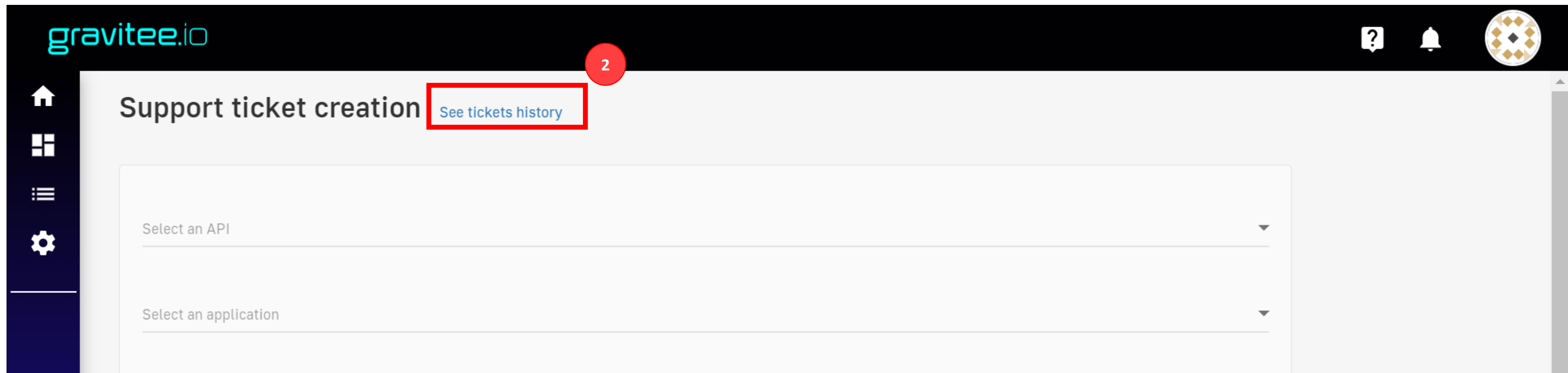
# Nouveau ticket

## Accéder à la saisie de ticket depuis le menu APIM Console



# Suivi de ticket

## Accéder à l'historique des tickets depuis le menu APIM Console



# Détails du ticket

## Accéder aux détails du ticket depuis l'historique des tickets depuis APIM Console

gravitee.io

?

🔔

🏠

🗄️

☰

⚙️

Tickets history

[Back to ticket creation](#)

Date ↓	Api	Application	Subject	
2020-10-28 11:31:44.320	Api1	Default application	My subject	<div><div>👁️</div><div>3</div></div>

15 ▼

1 - 1 of 1

<

>

# Organisation & Environnement



# Concepts

## Deux concepts s'appliquent au setup de l'API Management. L'organisation et l'environnement

La partie logique de l'entreprise qui fait le plus de sens au setup, par exemple le département ou l'entité. Dans le contexte de l'APIM, c'est le niveau auquel les configurations partagées pour les environnements sont gérées, comme :

- Cela permet également les opérations à travers tous les environnements gérés (comme les imports/exports d'API)

1

L'environnement dans une infrastructure IT, comme le développement ou la production. Il peut y avoir de multiples environnements liés à une organisation. Dans le contexte de l'APIM, c'est le workspace dans lequel les utilisateurs gèrent leurs APIs, applications et souscriptions. Un environnement supporte ses propres catégories, groupes, page de documentation et règles de qualités.

## Des environnements techniques comme TESTING / PREPROD / PROD

Dans le cadre de l'implémentation du projet gateway à un environnement correspond une instance du produit Gravitee

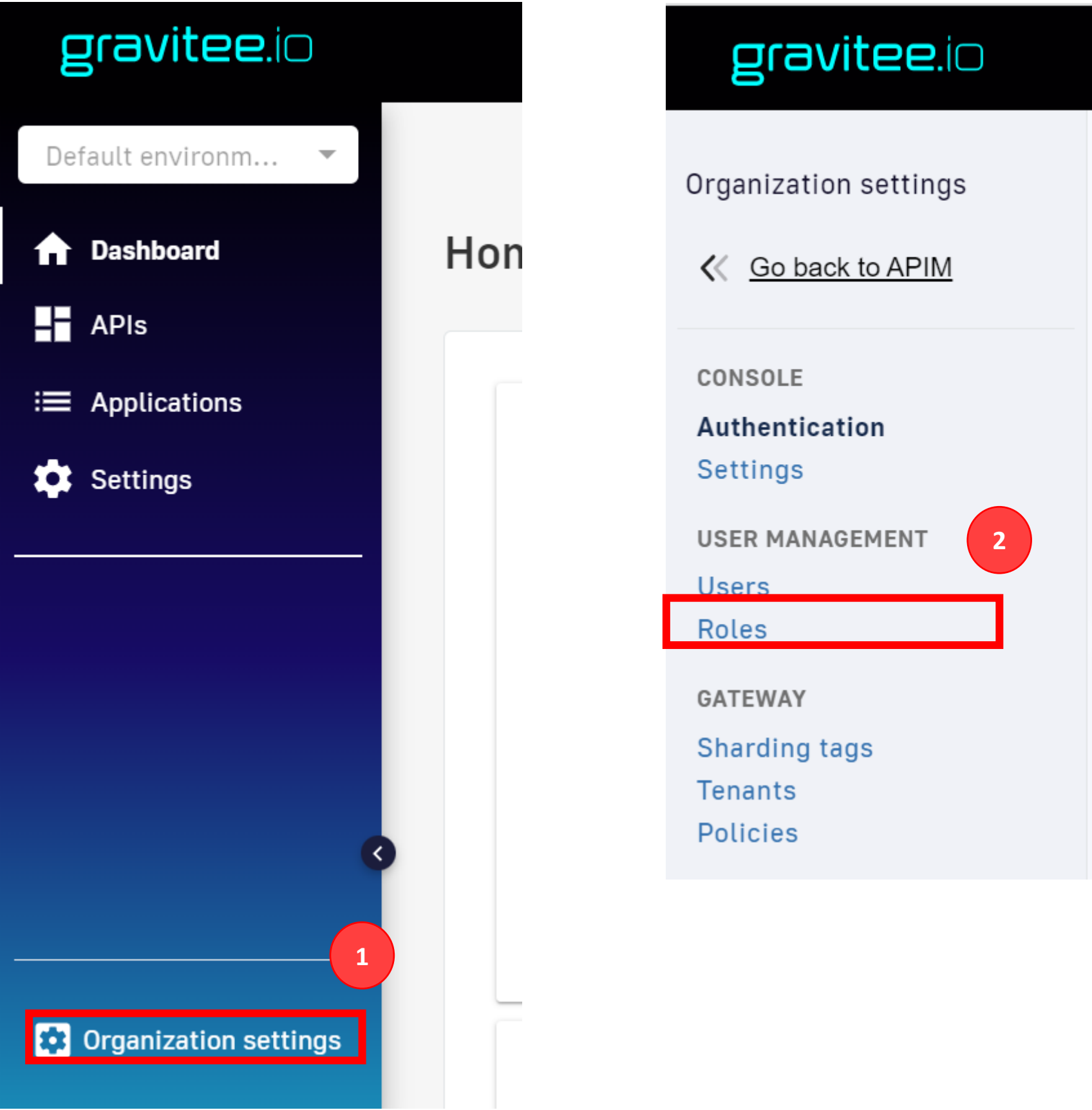


# Rôles et permissions

# Rôles et permissions

Accès à l'interface d'administration

MaaS ou MSP



## Résumé

Il est possible d'ajouter des rôles à chaque couche de Gravitee. Choisir avec attention dans quelle couche sera le nouveau rôle car cela peut impacter les droits dans les autres couches. Par exemple un ADMIN dans la couche organization aura des droits dans environnement, API et Application. Tandis qu'un ADMIN dans Application n'aura pas les droit dans les couche au dessus.

Dans le cas de l'implémentation du projet Gateway, aucune personnalisation des Roles n'a été opérée.

# Rôles et permissions

Ajouter un rôle

MaaS ou MSP

gravitee.io

?

🔔

Organization settings

<< [Go back to APIM](#)

CONSOLE

[Authentication Settings](#)

USER MANAGEMENT

[Users](#)

**Roles**

GATEWAY

[Sharding tags](#)

Roles

Organi...

Enviro...

API

Applic...

Organization

+ Add a role

ADMIN

System

System Role. Created by Gravitee.io

USER

Default

Default Organization Role. Created by Gravitee.io.

Commencer par choisir la couche dans laquelle ajouter le rôle, puis cliquer sur ‘Add a role’

Programme Mon Compte Mobilité, porté par Capgemini et son porteur associé La Fabrique des Mobilités



# Rôles et permissions

Ajouter un rôle

MaaS ou MSP

Manage CRUD (Create, Read, Update, Delete) permissions for this role in the Organization scope.

Role name \*

The name cannot be changed after it has been created.

Role description

Default role☐

Indiquer le nom du rôle et sa description. Il est possible de choisir si un rôle et un rôle par défaut. Si tel est le cas alors ce rôle sera appliqué à tous nouveaux membres s’inscrivant dans la couche organization.