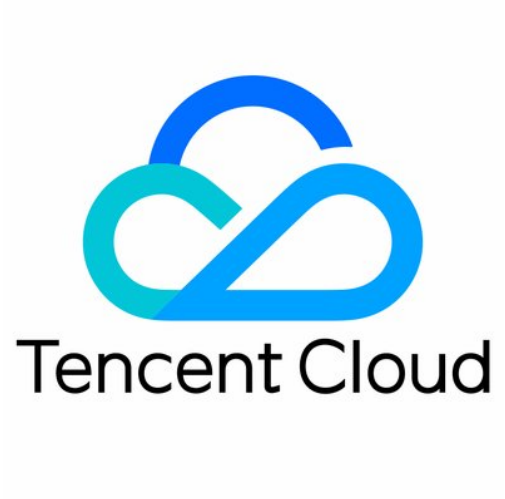
# API Gateway

# Usage Plan

# Product Documentation



# Contents

# Usage Plan Overview

Last updated：2023-12-22 09:52:59

API Gateway uses usage plans to control the authentication, request traffic, quotas, and API user permissions after a service is published.

Currently, the content that can be adjusted and controlled by a usage plan includes:

Authentication and security control

Traffic control

A usage plan will take effect after it is bound to a service environment.

Multiple usage plans can be bound to the same service environment, and one usage plan can be bound to multiple service environments.

**Note：**

Two or more usage plans bound to the same key cannot be bound to the same environment in the same service. Similarly, if two or more usage plans have been bound to the same environment in the same service, they cannot be bound to the same key.

# Working with a Usage Plan

Last updated：2023-12-22 09:53:14

## Scenarios

To call a service after it is published, you need to create a key-value pair secret and a usage plan and bind them to the service environment.
This document describes how to configure a user-specific usage plan and make it available to the users.

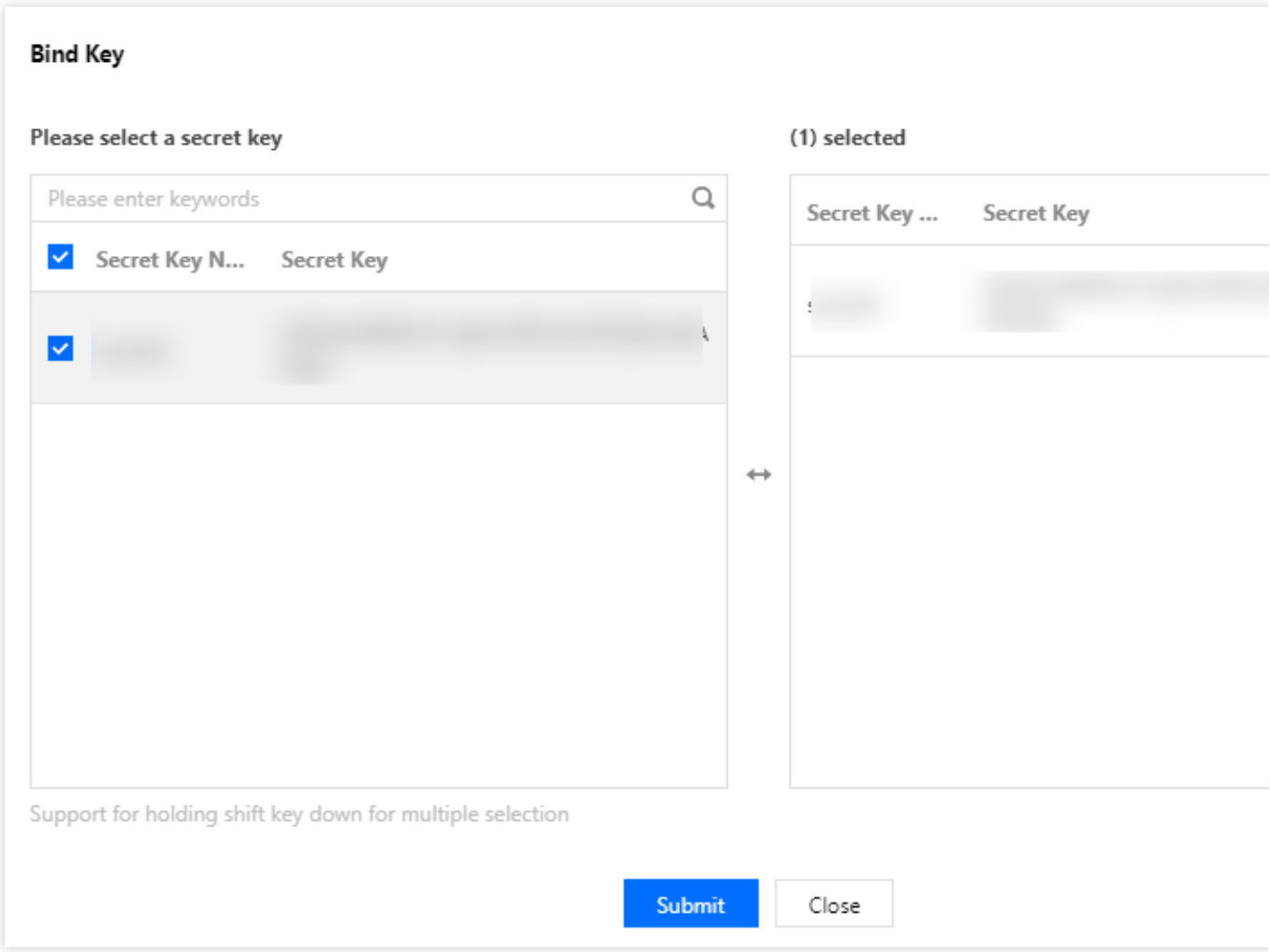
## Prerequisite

1. Create a service and create and debug an API.
2. Publish the service to an environment, such as the release environment.

## Directions

### Creating a key-value pair secret

1. Log in to the API Gateway console, and click **Application** on the left sidebar to enter the application management page.
2. On the application management page, click **Secret** on the top to open the secret management page.
3. Click **Create**, select the secret type and complete the following information.
Auto-generated
Custom secret
Enter the secret name.
Secret name: Up to 50 characters ([a-z], [A-Z], [0-9] and [_])
Enter the secret name, SecretId and SecretKey.
Secret name: Up to 50 characters ([a-z], [A-Z], [0-9] and [_-])
SecretId: 5-50 characters ([a-z], [A-Z], [0-9] and [_-])
SecretKey: 10-50 characters ([a-z], [A-Z], [0-9] and [_-])
4. Click **Submit** to generate a secret or save the custom key-value pair secret (SecretId and SecretKey).

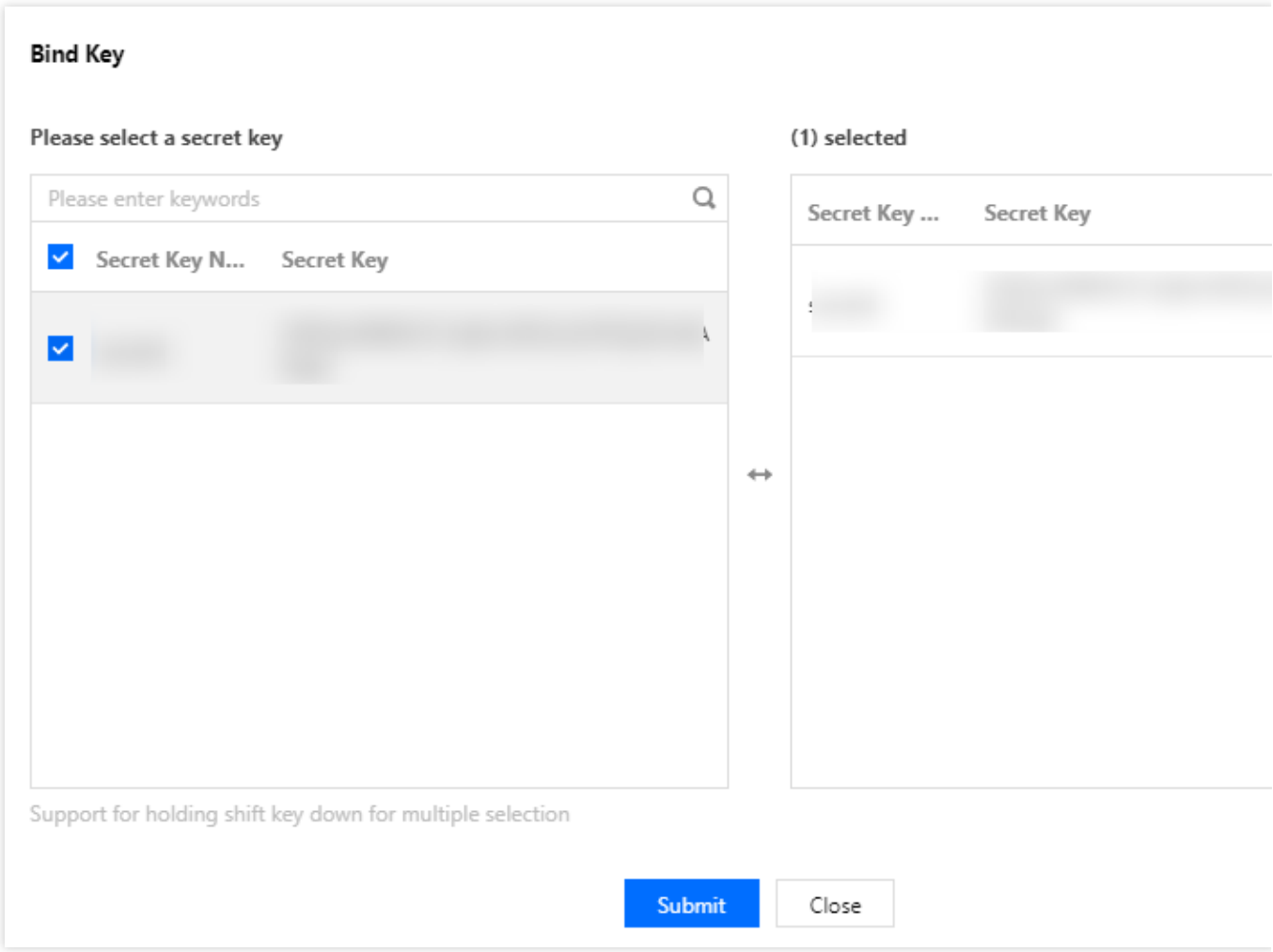



## Creating a usage plan

1. On the left sidebar, click Usage Plan to enter the usage plan list page.
2. Click **Create** in the top-left corner and enter the configuration information as prompted.
3. Click **Submit** to complete the creation.

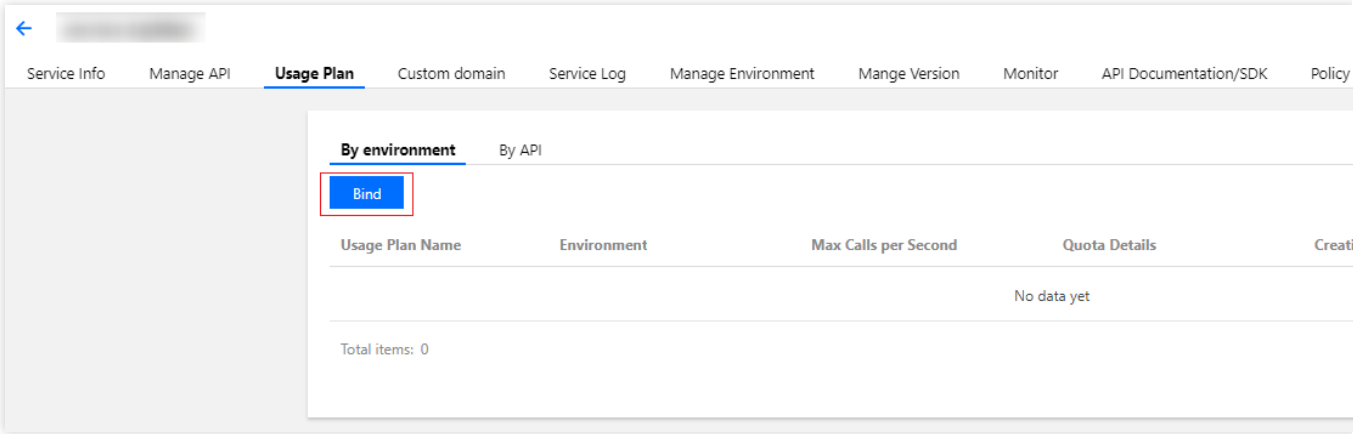
## Binding usage plan to secret

1. On the Usage Plan page, click the ID of the target usage plan to enter the usage plan details page.
2. On the usage plan details page, click **Bind Key**.
3. Check the `SecretId` to be bound and click **Submit** to complete the binding.




## Binding a usage plan with a service environment

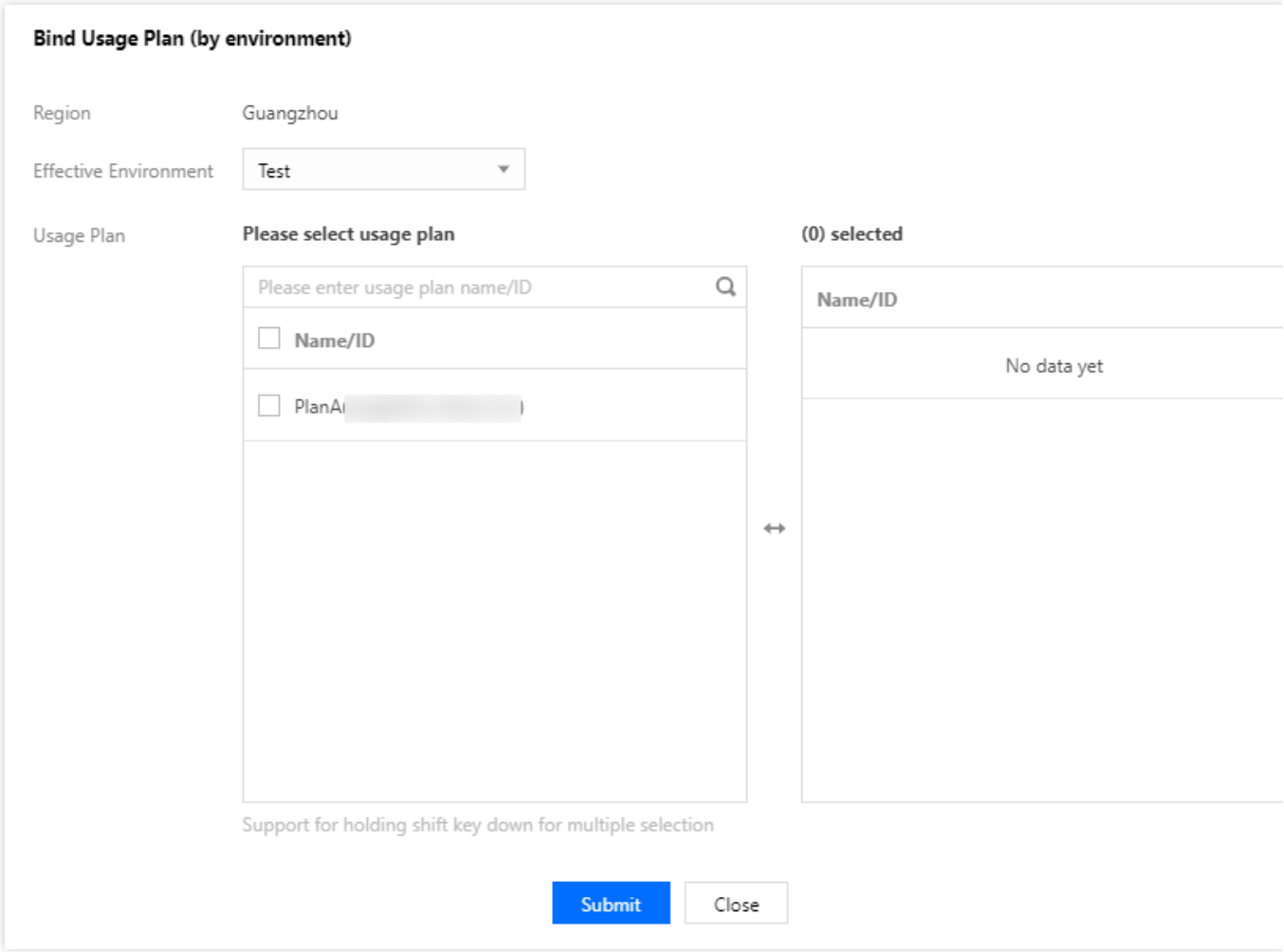
1. Select a created service on the Service list page, switch to the **Usage Plan** tab, and click **Bind**.




2. In the usage plan binding window, select an effective environment and usage plan to be bound.

Effective environments: publish, pre-publish, and testing

3. Click **Submit** to complete the binding.




**Note:**

Usage plans bound with the same key-value pair cannot be bound to the same environment.

Now you can share the SecretId and SecretKey to the end user. The end user can use the provided `SecretId` and `SecretKey` through the second-level domain name of the service (or a bound private domain name) to access the APIs published in the service.

# Traffic Control

Last updated：2023-12-22 09:53:31

You can limit the maximum number of calls under a usage plan by setting the QPS in it and binding a key.
For example, if you create a `secret_id` and `secret_key` pair and a usage plan with 1,000 QPS, bind the `secret_id` and `secret_key` pair to the usage plan, and bind the usage plan to the environment where you need to limit the traffic, such as the release environment, then an API in the release environment can be called by a user with the `secret_id` and `secret_key` pair at a frequency of up to 1,000 QPS.
Currently, up to 2,000 QPS can be set for each usage plan. Because the architecture of API Gateway is designed to be highly available, forwarded requests will be processed by different underlying nodes. If the traffic control value is too small (such as less than 5 QPS), there will be a certain probability that traffic control will be inaccurate, and the actual number of requests allowed to pass will be slightly greater than the set value.