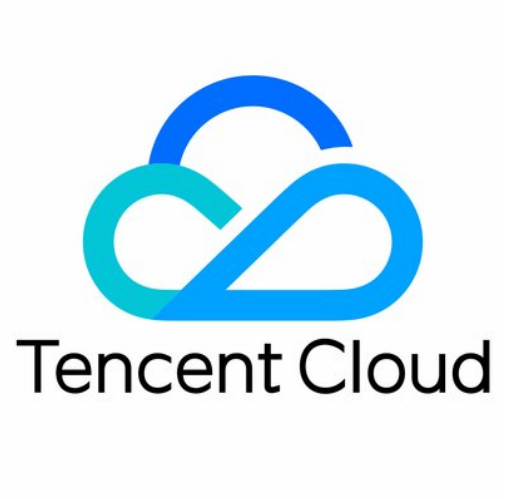
Tencent Push Notification Service

Users and Permissions

Product Documentation



Contents

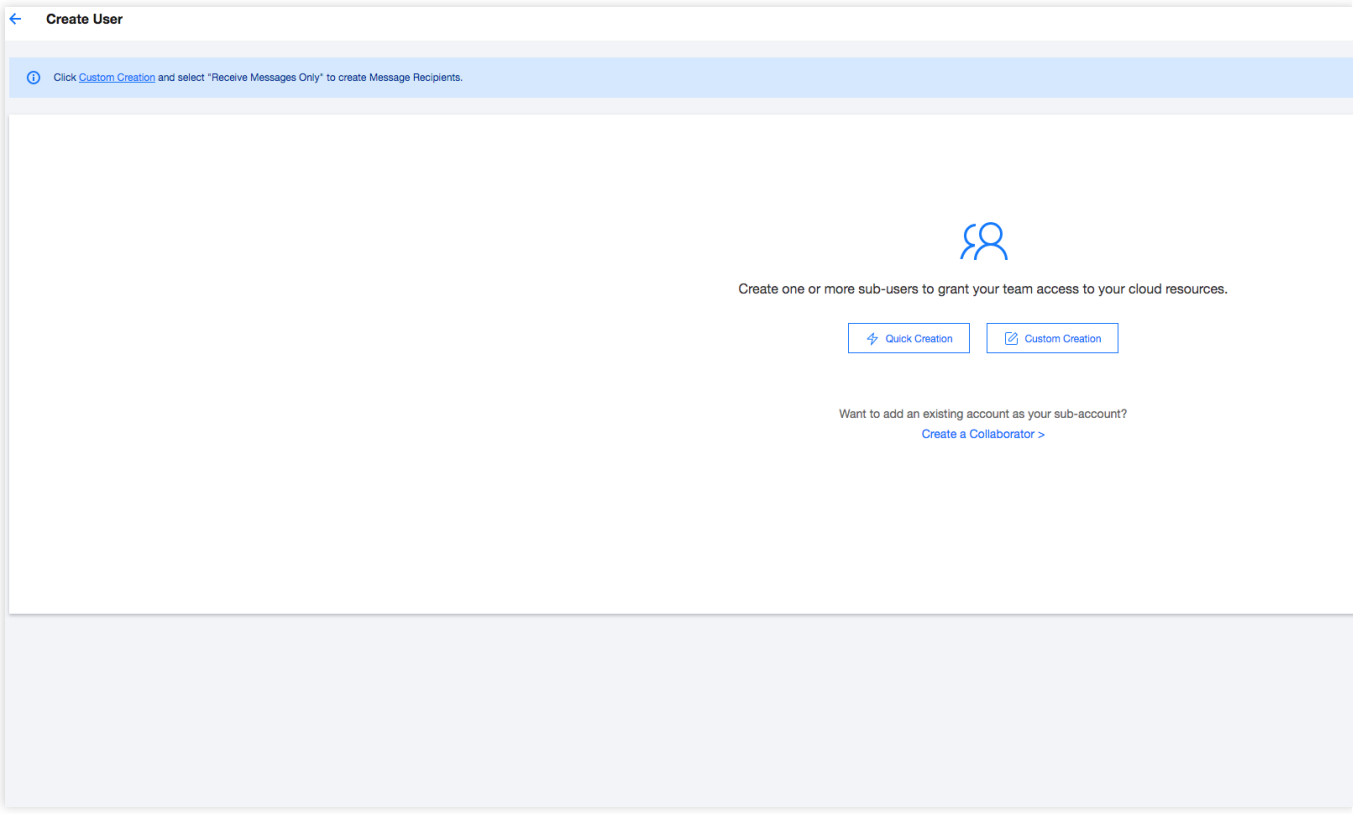
Users and Permissions Quick Configuration

Last updated：2024-01-16 17:43:54

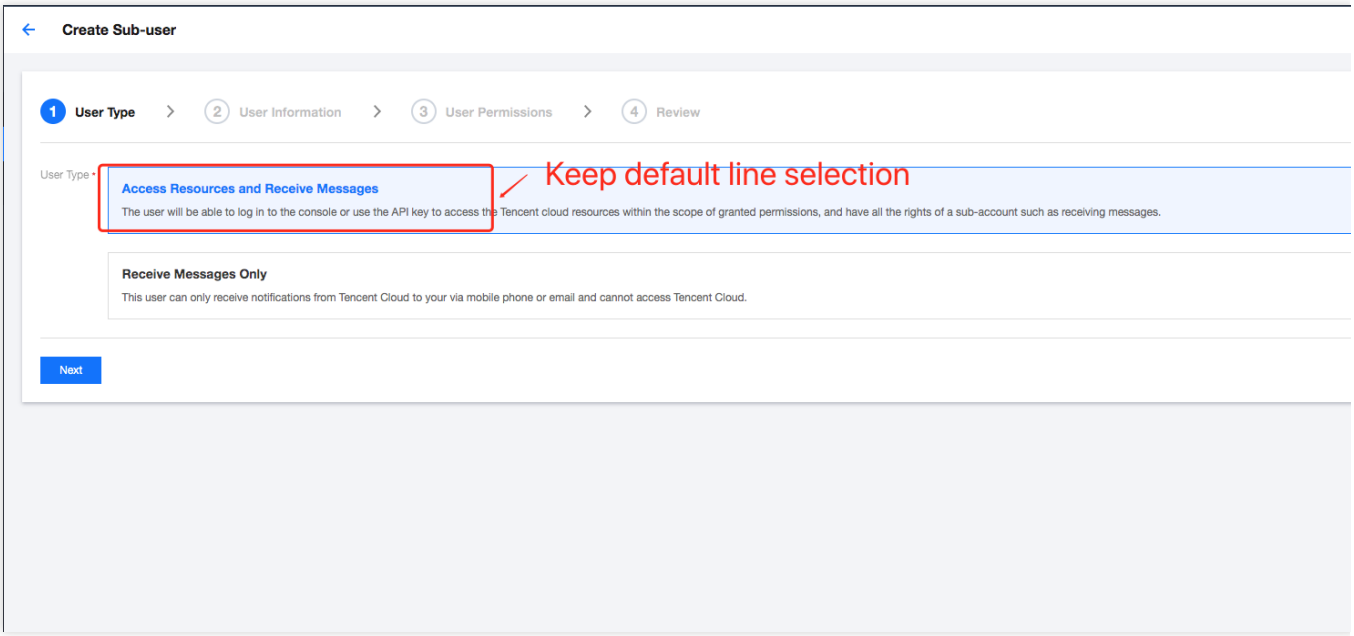
This document describes how to create and authorize sub-users. If you have never used Tencent Cloud Access Management (CAM), read this document for more information on the configuration.
Tencent Push Notification Service uses CAM for permission management. You need to authorize applications, create sub-users, and grant application permissions to the sub-users. For detailed directions, see the following sections.

Creating a Sub-User

1. Go to the CAM console and click **Create User**.



2. Click **Custom Creation** to enter the **Create Sub-user** page (this example is based on the custom creation method).

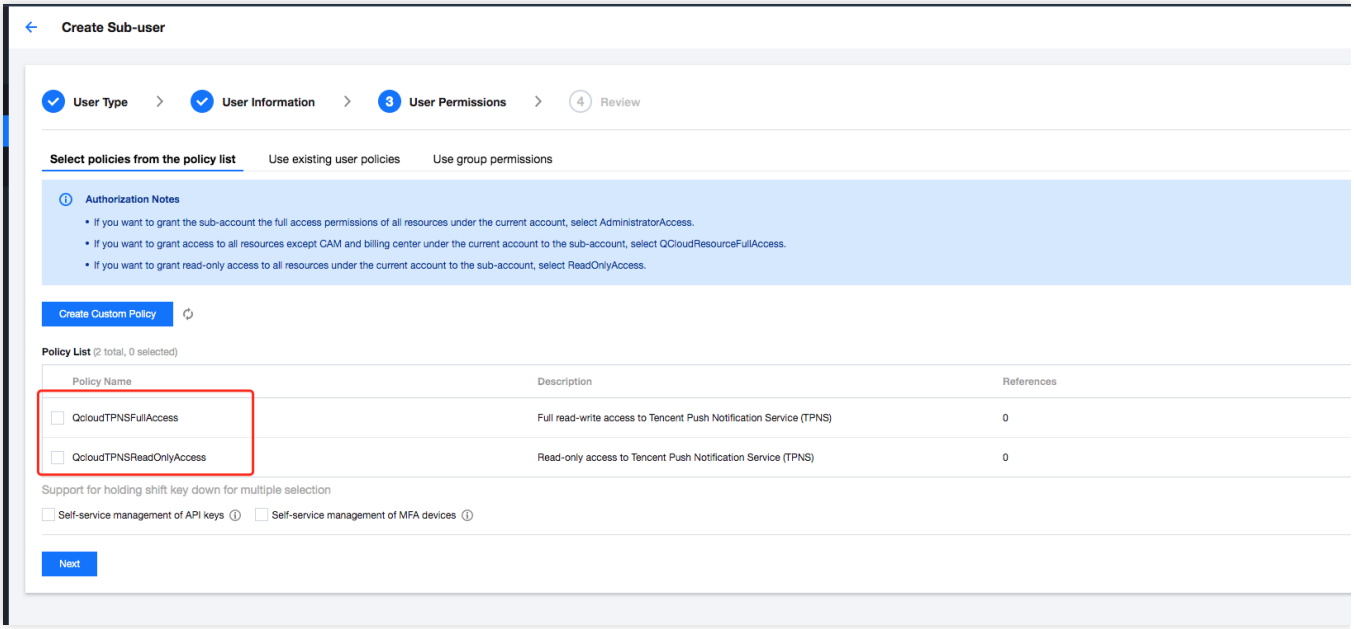


3. Configure the login information of the sub-user as instructed and grant the sub-user application permissions in the **User Permissions** step.

Granting Application Permissions

Granting permissions of all applications in a centralized manner

1. Continue with the **User Permissions** page mentioned in the previous step.

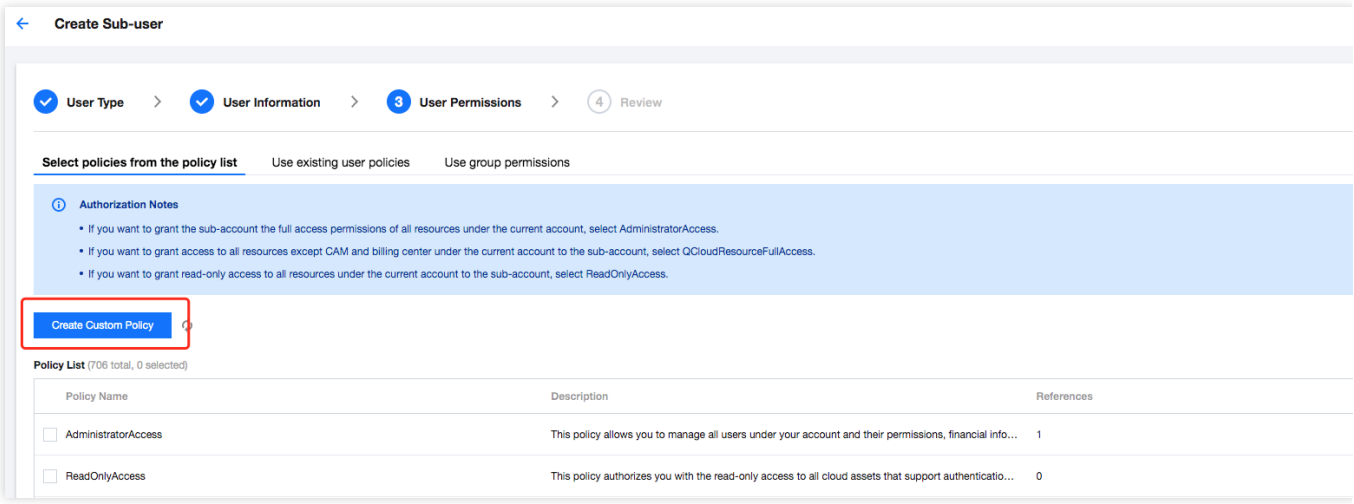


2. Enter **Tencent Push Notification Service** in the search box. In the search results, there are two default preset permissions as listed below:

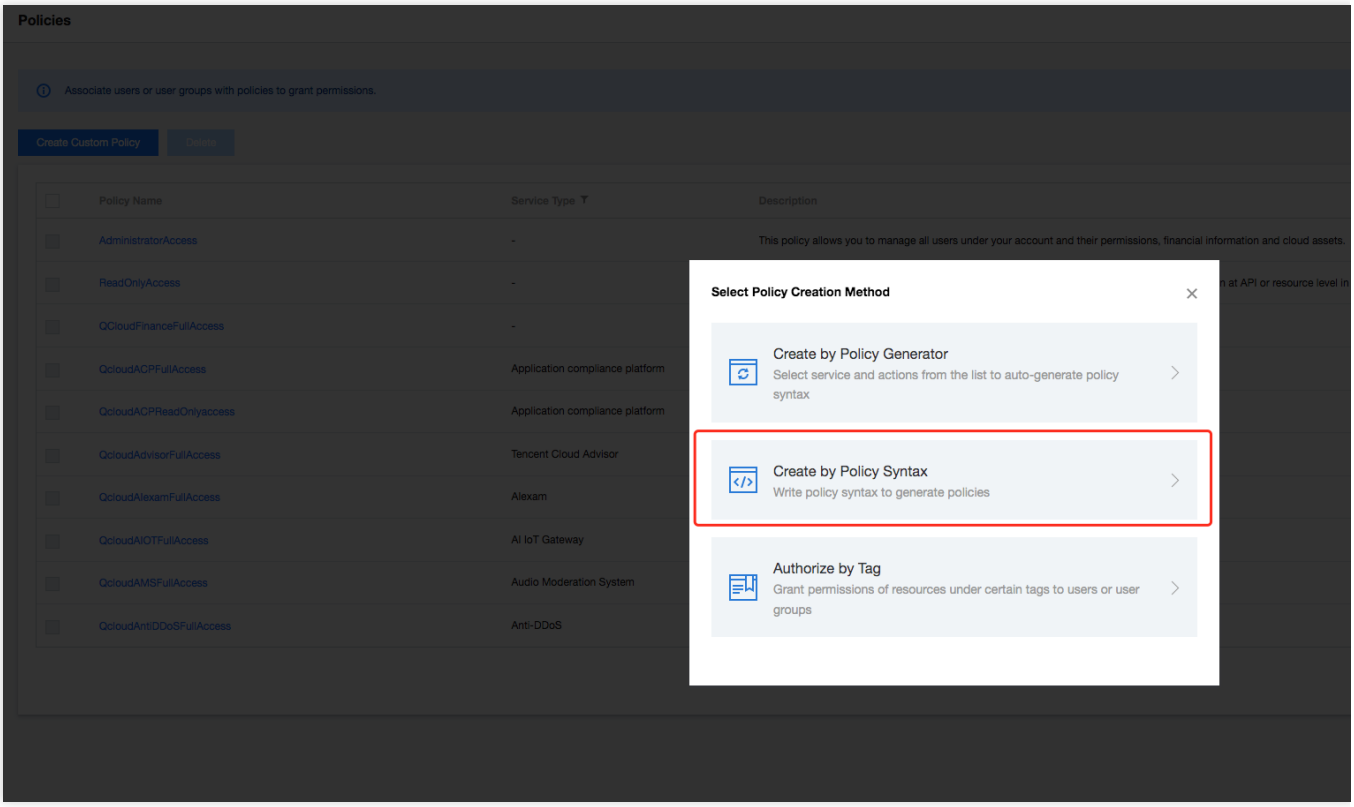
Policy Name	Permission Scope
QcloudTPNSFullAccess	All permissions on all the applications under the root account
QcloudTPNSReadOnlyAccess	Data read and push permissions on all applications under the root account

Granting permissions of selected applications

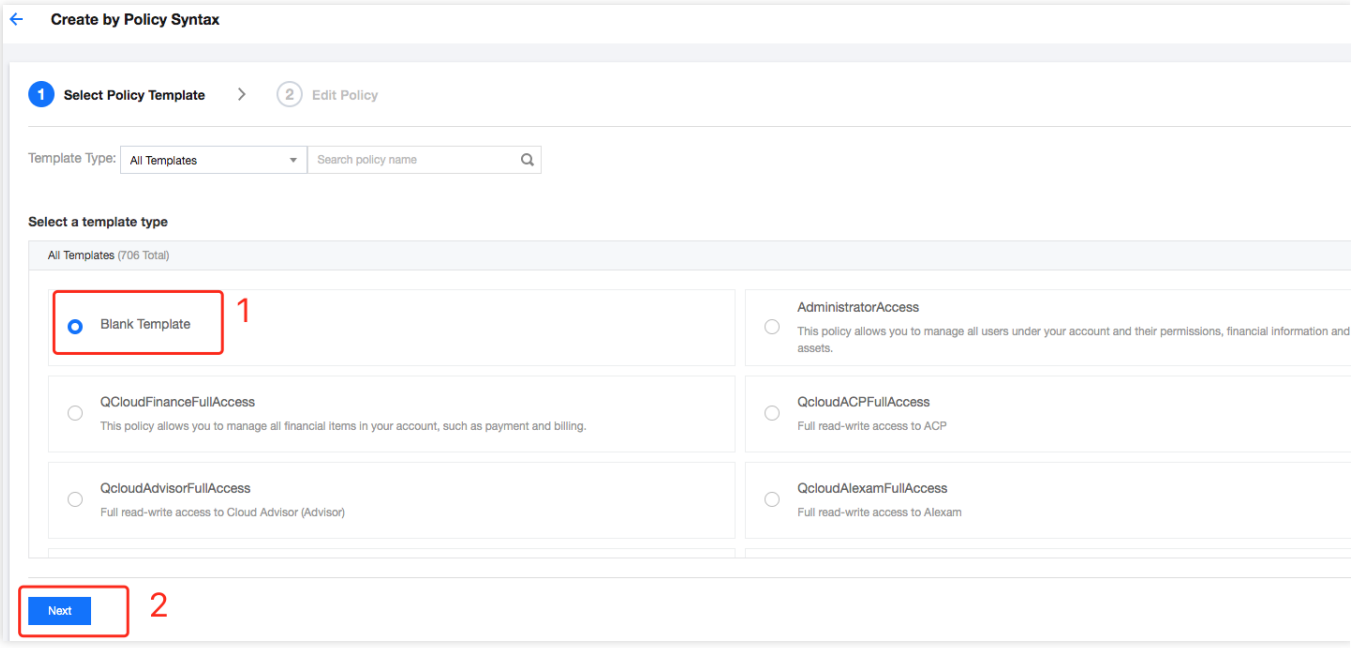
1. Click **Create Custom Policy**.



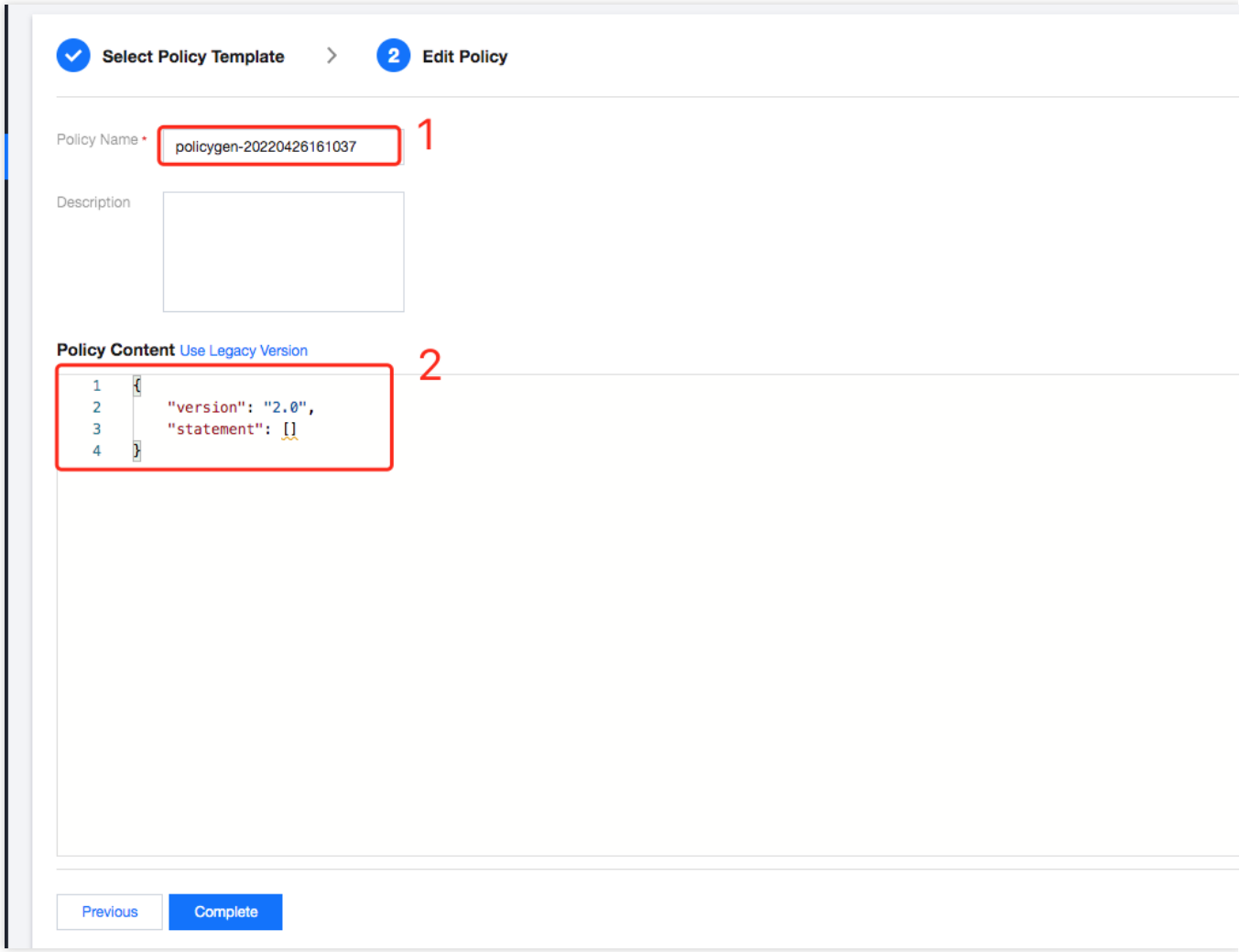
2. On the displayed page, select **Create by Policy Syntax**.



3. Select **Blank Template**.



4. Click **Next** to enter the syntax creation page.

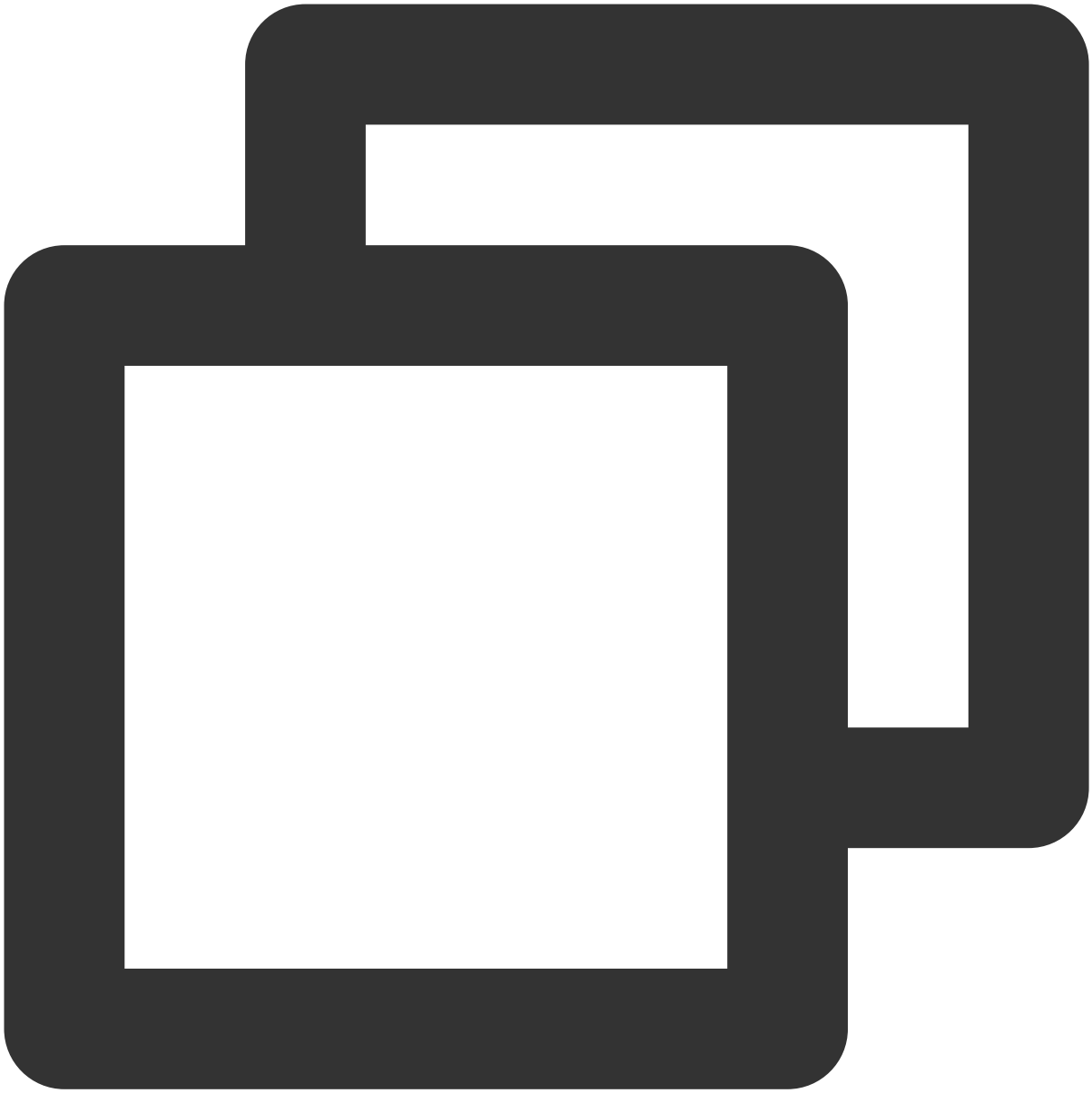


Note:

Enter an easy-to-remember policy name.

Copy the code provided in this document and replace the account ID and Access_ID in it with your own account ID and Access_ID, which can be found on the account information page under the current root account and the Tencent Push Notification Service product management page in the console respectively.

Copy the following syntax code:



```
{
 "version": "2.0",
 "statement": [
     {
         "action":[
             "tpns:Describe*",
             "tpns:CancelPush",
             "tpns:DownloadPushPackage",
             "tpns:CreatePush",
             "tpns:UploadPushPackage"
         ],
```

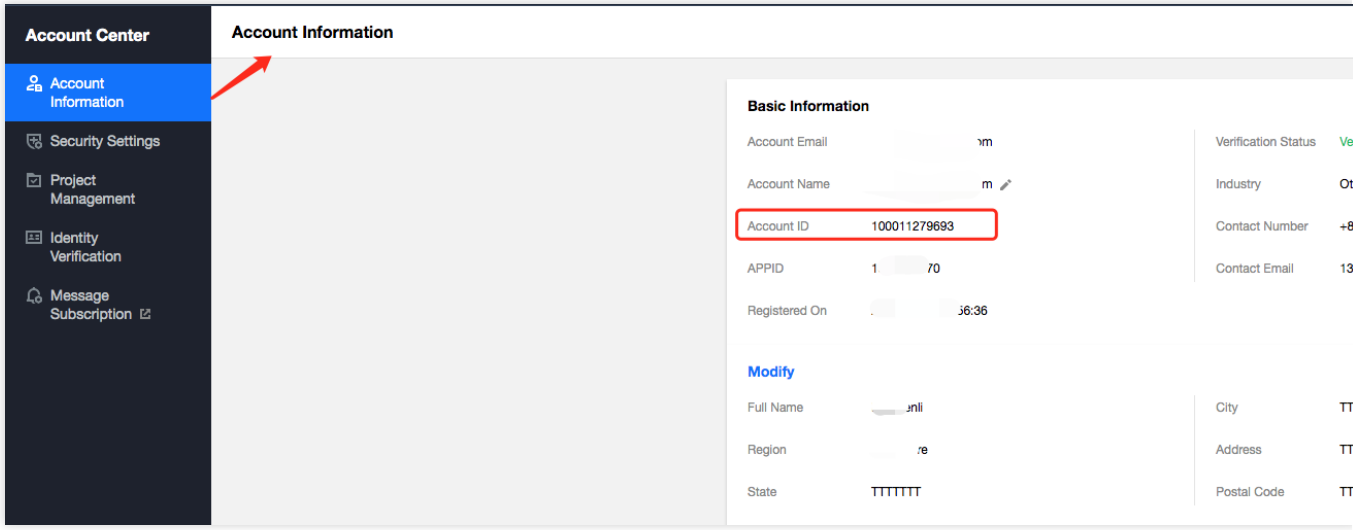
```
            "resource": [
                "qcs::tpns::uin/1000000000:app/1500000000"
            ],
            "effect": "allow"
        },
        {
            "action":[
                "tpns:Describe*"
            ],
            "resource": [
                "qcs::tpns::uin/1000000000:/*"
            ],
            "effect": "allow"
        }

    ]
}
```

Replace parameters in the syntax code as follows:

Replace the ID of the root account: enter the Account Information page under the current root account, copy the account ID, and replace `1000000000` in the syntax above with it.

Note:

If your current login account is a collaborator or sub-account, you need to get the account ID from the owner of the root account that grants you permissions.



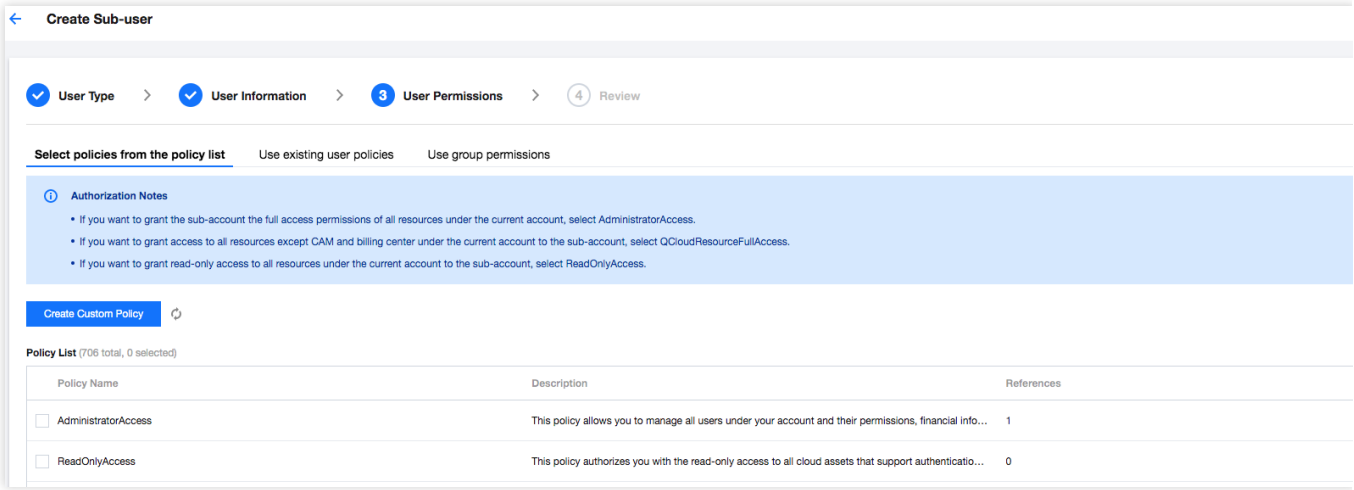
Replace the application `Access_ID` : go to the Product Management page in the Tencent Push Notification Service console, copy the `Access_ID` of the application whose permissions you want to grant, and replace `1500000000` in the syntax above with it. If you want to grant permissions of multiple applications, you can change `resource` to:

`"qcs::tpns::uin/1000000000:app/{Application Access_ID 1}"`, `"qcs::tpns::uin/1000000000:app/{Application Access_ID 2}"`

Note:

Please delete "{" and "}" in actual use. For detailed directions, please see Advanced Custom Configuration.

5. Go back to the user creation page.



Search for the created policy by name, select it, click **Next**, and click **Complete**.

6. After the permission configuration, you can select **Sub-User Login** on the login page to verify the account permissions.

Advanced Custom Configuration

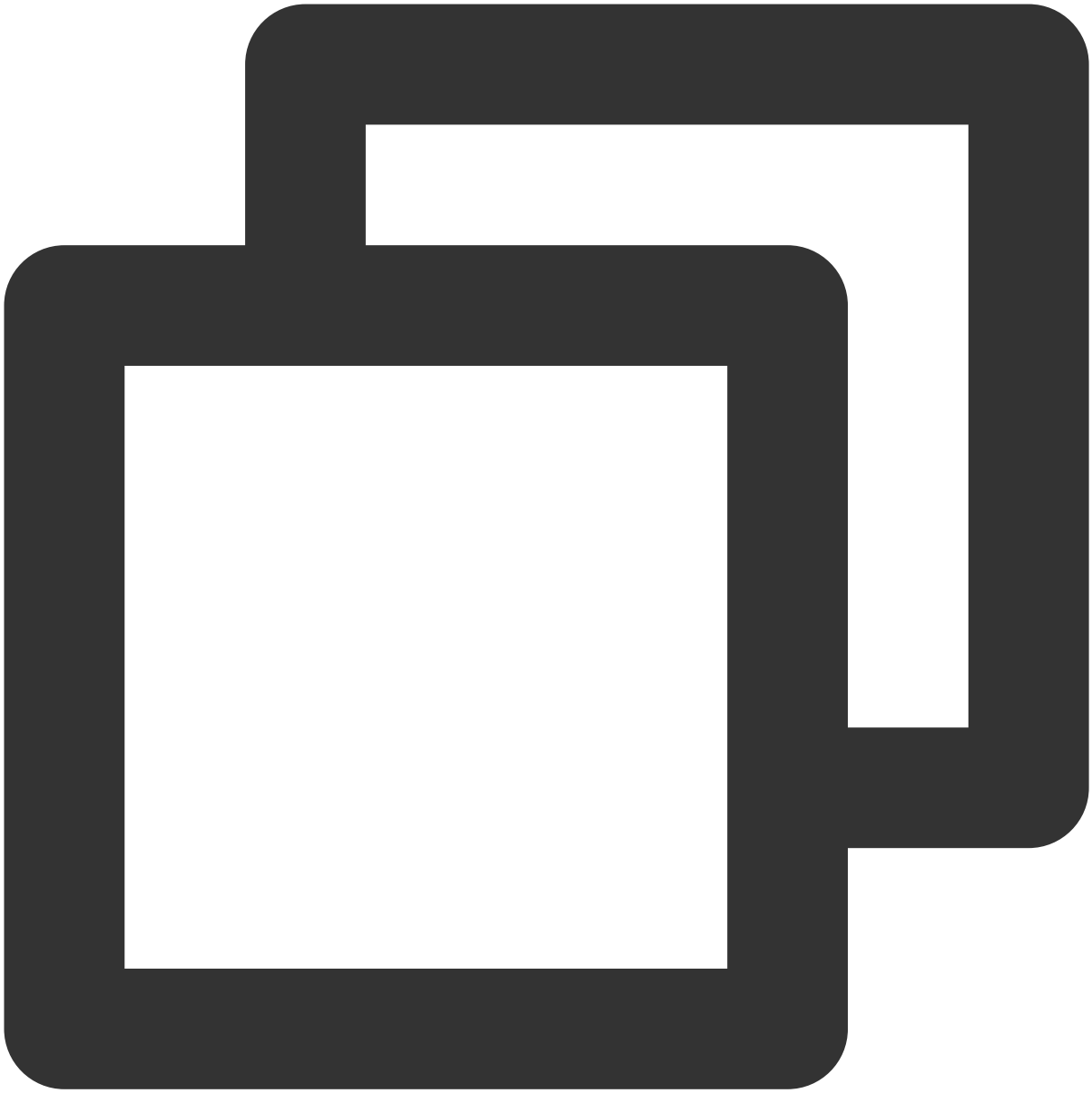
Last updated：2024-01-16 17:43:54

Overview

If you use the Tencent Push Notification Service service in Tencent Cloud, and the service is managed by different users sharing your Tencent Cloud account key, the following problems may occur:
The risk of your key being compromised is high since multiple users are sharing it.
Your users might introduce security risks from misoperations due to the lack of user access control.
You can allow different users to manage different services through sub-accounts to avoid the above problems. By default, a sub-account does not have permission to use a Tencent Push Notification Service service or related resources. Therefore, you need to create a policy to grant the required permission to the sub-account.
Tencent Cloud's Cloud Access Management (CAM) is a web service that helps you manage the access permissions for resources under your Tencent Cloud accounts. With CAM, you can create, manage, or terminate users (groups), and manage identities and policies to allow specific users to access and use specific Tencent Cloud resources.
You can use CAM to associate a user/user group with a policy, which allows/denies the user to use specified resources to perform specified tasks. For CAM policy basics, please see Syntax Logic. For the use of CAM policies, please see Policy.
Note:
If you do not need to manage access permissions to Tencent Push Notification Service resources for sub-accounts, you can skip this part. This will not affect your understanding and use of other parts of the documentation.

Policy Syntax Description

A CAM policy must authorize or deny the use of one or more Tencent Push Notification Service operations. At the same time, it must specify the resources that can be used for the operations (which can be all resources or partial resources for certain operations). For Tencent Push Notification Service operations that do not support resource-level authorization, you need to specify the authorized object as all resources.
CAM policy syntax description:



```
{
        "version":"2.0",
        "statement":
        [
            {
                "effect":"effect",
                "action":["action"],
                "resource":["resource"],
                 "condition": {"key":{"value"}}
            }
        ]
```

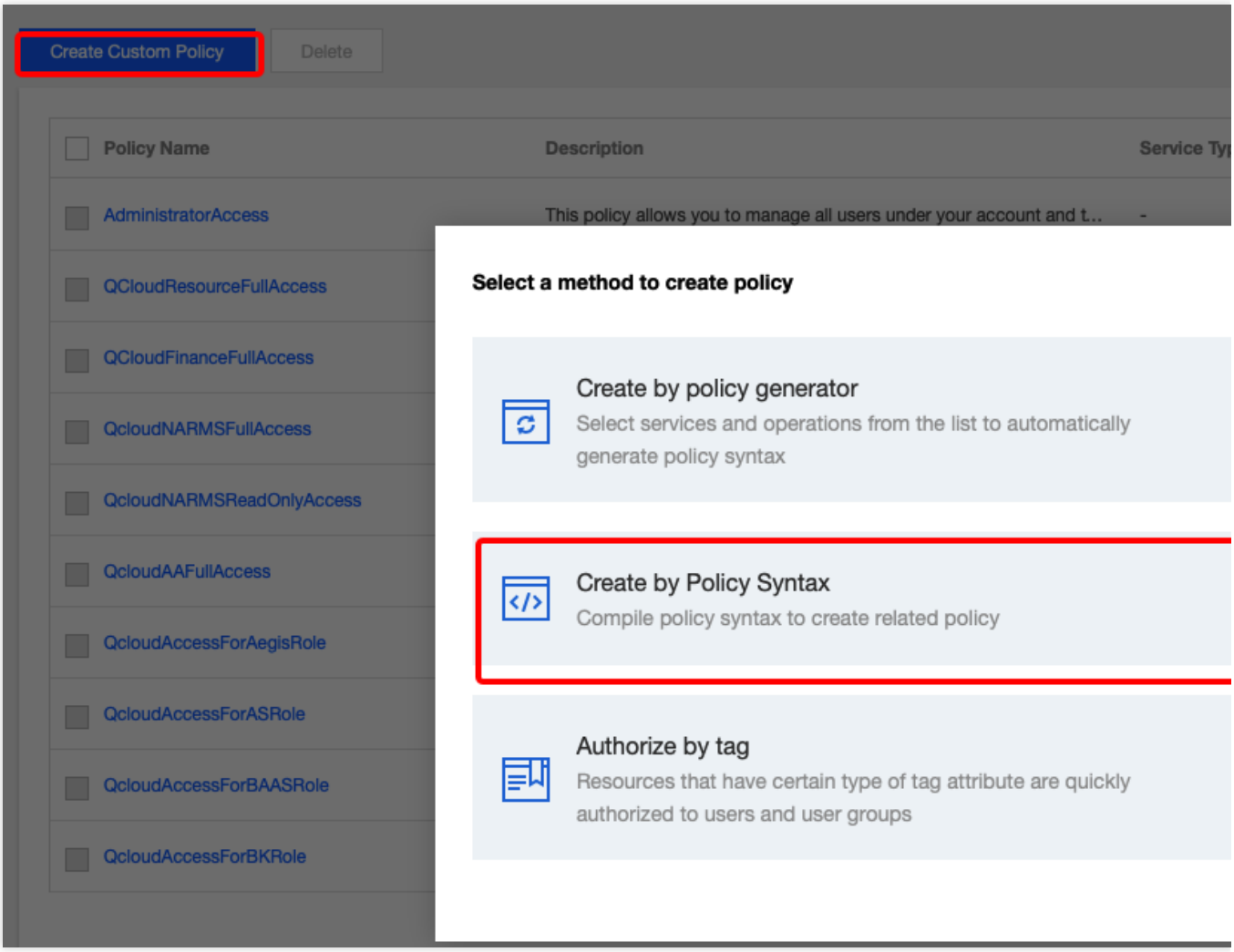
```
}
```

Parameter description:

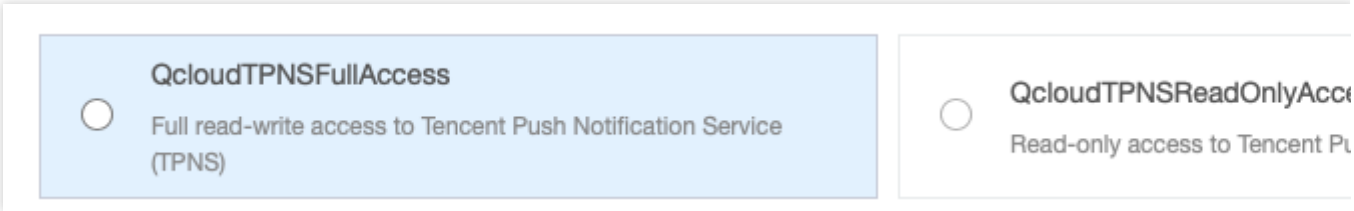
Parameter	Required	Description
version	Yes	Version number. Currently, only "2.0" is supported.
statement	Yes	This element describes the details of one or more permissions. It contains a permission or permission set of other elements such as `effect`, `action`, `resource`, and `condition`. One policy has only one statement. An `action` (operation) describes an allowed or denied operation, which can be an API or a feature set (a set of specific APIs prefixed with `permid`).
resource	Yes	The specific resource. A resource is described in a six-segment format. Detailed resource definitions vary with the products. For more information about how to specify a resource, please see the documentation of the corresponding product.
condition	No	The condition for the policy to take effect. A condition consists of the operator, action key, and action value. A condition value may be the time, IP address, etc. Some services allow you to specify additional values in a condition.
effect	Yes	Describes whether the statement result is "allowed" (`allow`) or "explicitly denied" (`deny`).

Creating Policy and Granting Permissions

Two types of system-level policies are preset for you to quickly grant permissions. You can go to the console > Cloud Access Management > Policies, click **Create Custom Policy**, and select **Create by Policy Syntax**, as shown below:



On the **Create by Policy Syntax** page, you can search and find two preset policy templates, which grants full access and read-only access, respectively (you can view the list of specific permissions during policy creation). You can select a template and edit it or create a blank template.

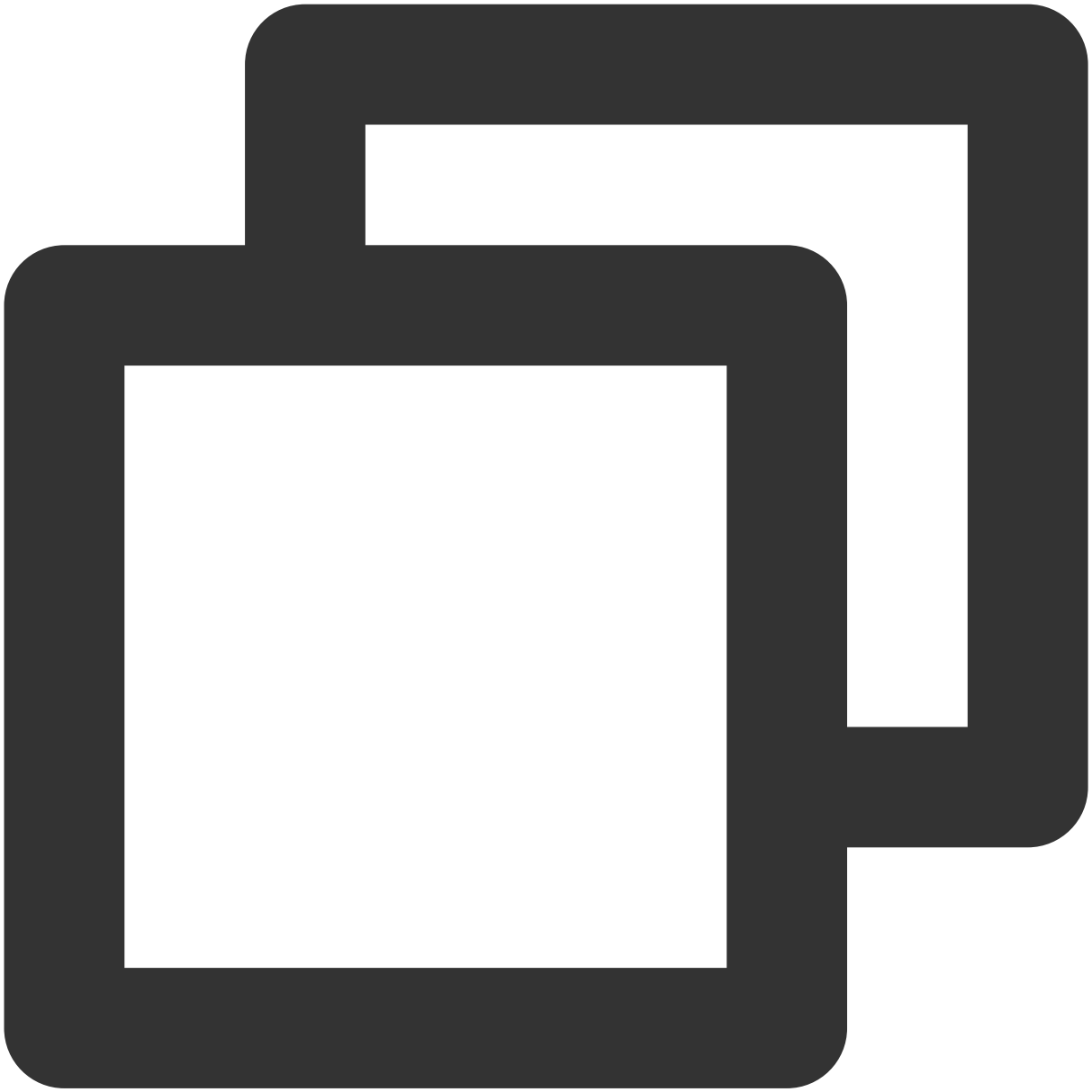


After creating a policy, you can find it on the Policies page in the CAM console and associate it with a sub-user to complete the permission configuration.

This document describes how to perform CAM authorization in Tencent Push Notification Service.

Authorizable Tencent Push Notification Service Resources

Resource-level permission can be used to specify which resources a user can manipulate. The type of resources that can be authorized in Tencent Push Notification Service is "app", that is, you can grant resource-level permissions in CAM at the app granularity. The resource description method is as follows:



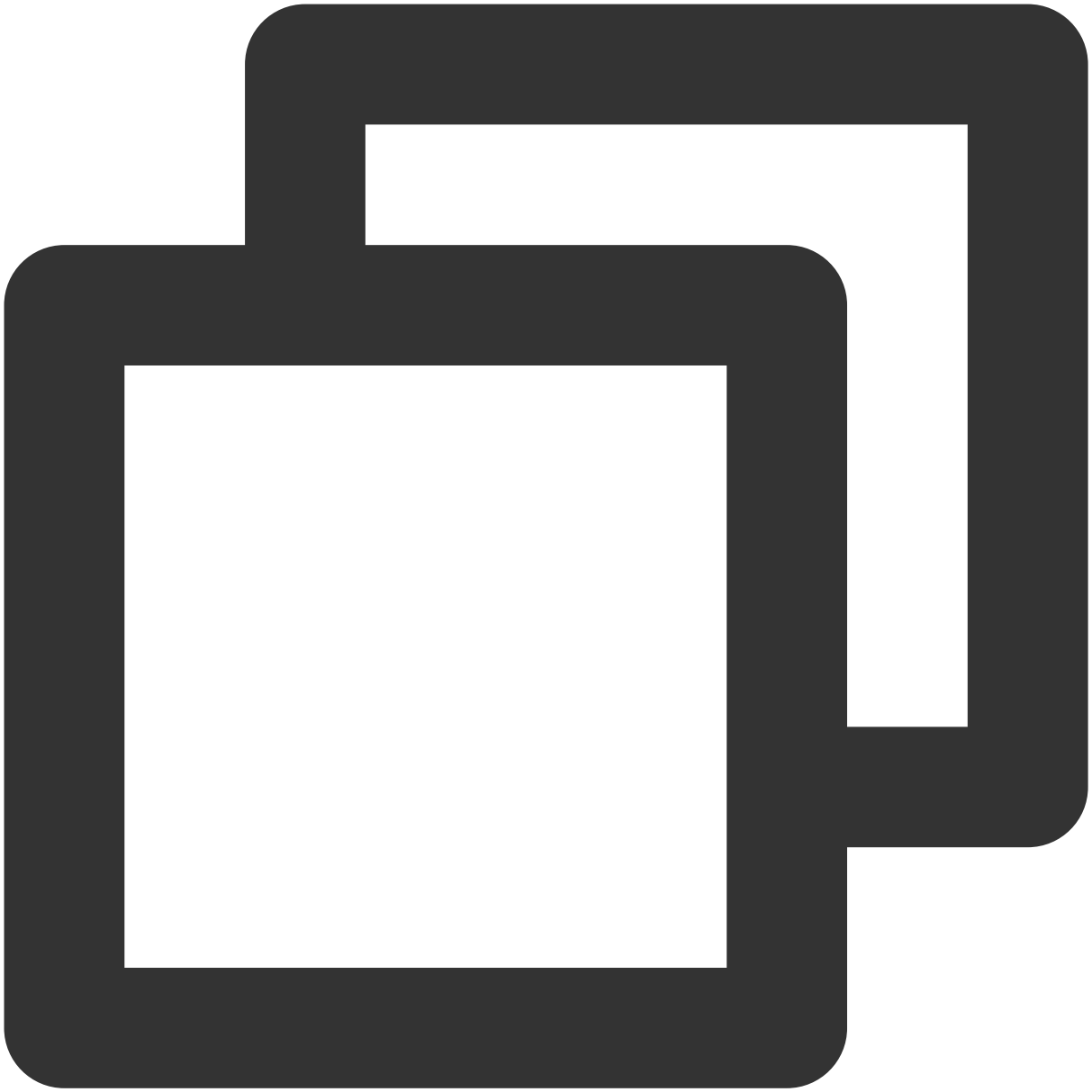
```
qcs::tpns::uin/1000000000:app/*
```

Here, `*` indicates all resources at the app granularity, which can be replaced with the `Access ID`. You can find the app's `Access ID` in the Product Management module in the Tencent Push Notification Service Console. For the `uin`, get the account ID on the Account Info page in the console and replace the `uin` with it (such as `1000000000`, which is a sample Tencent Cloud ID of a root account).

When authorizing multiple resources, separate them with commas.

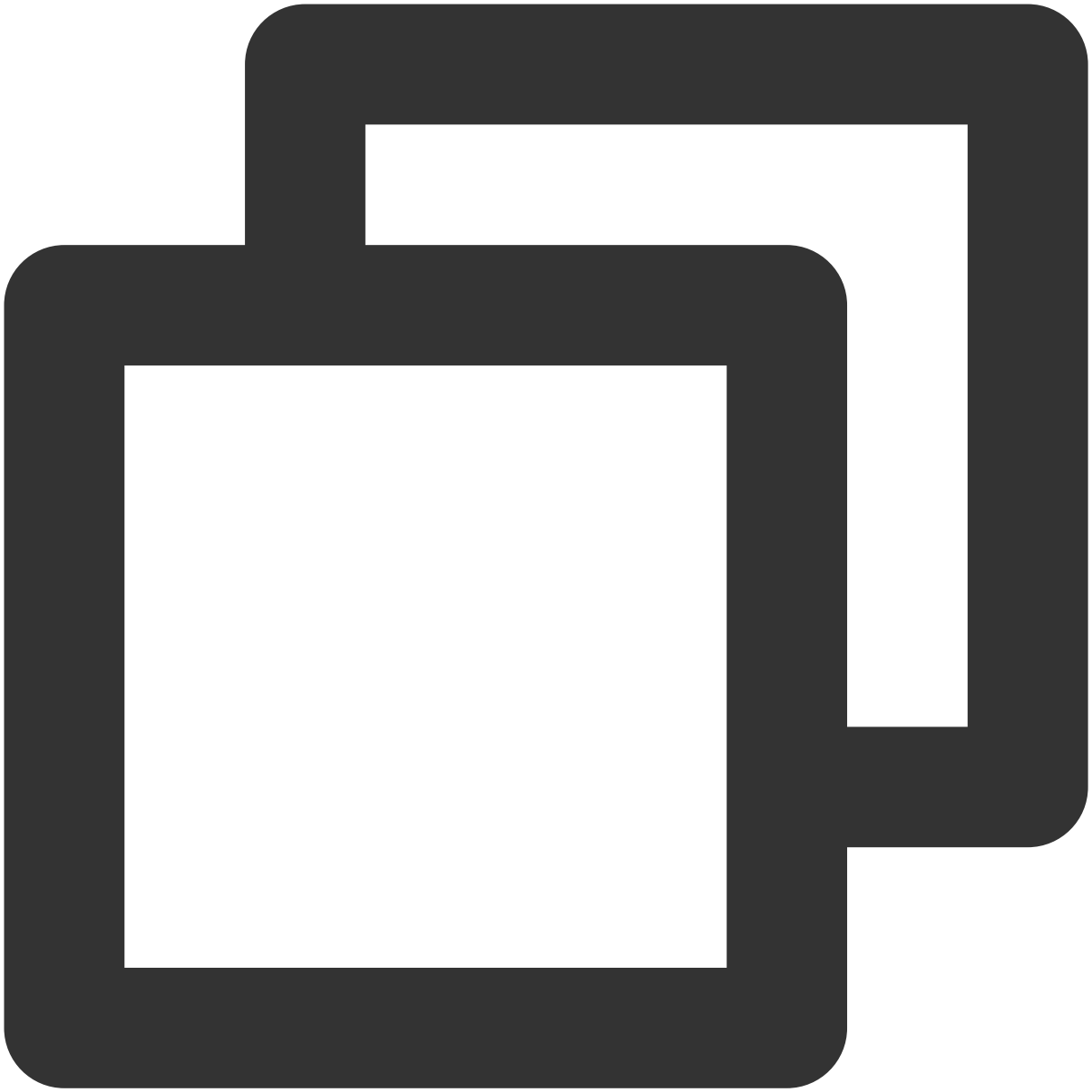
Tencent Push Notification Service Operations That Can Be Authorized

In a CAM policy statement, you can specify any API operation from any service that supports CAM. APIs prefixed with `name/tpns:` should be used for Tencent Push Notification Service, such as `name/tpns:CreateProduct` .
To specify multiple operations in a single statement, separate them with commas as shown below:



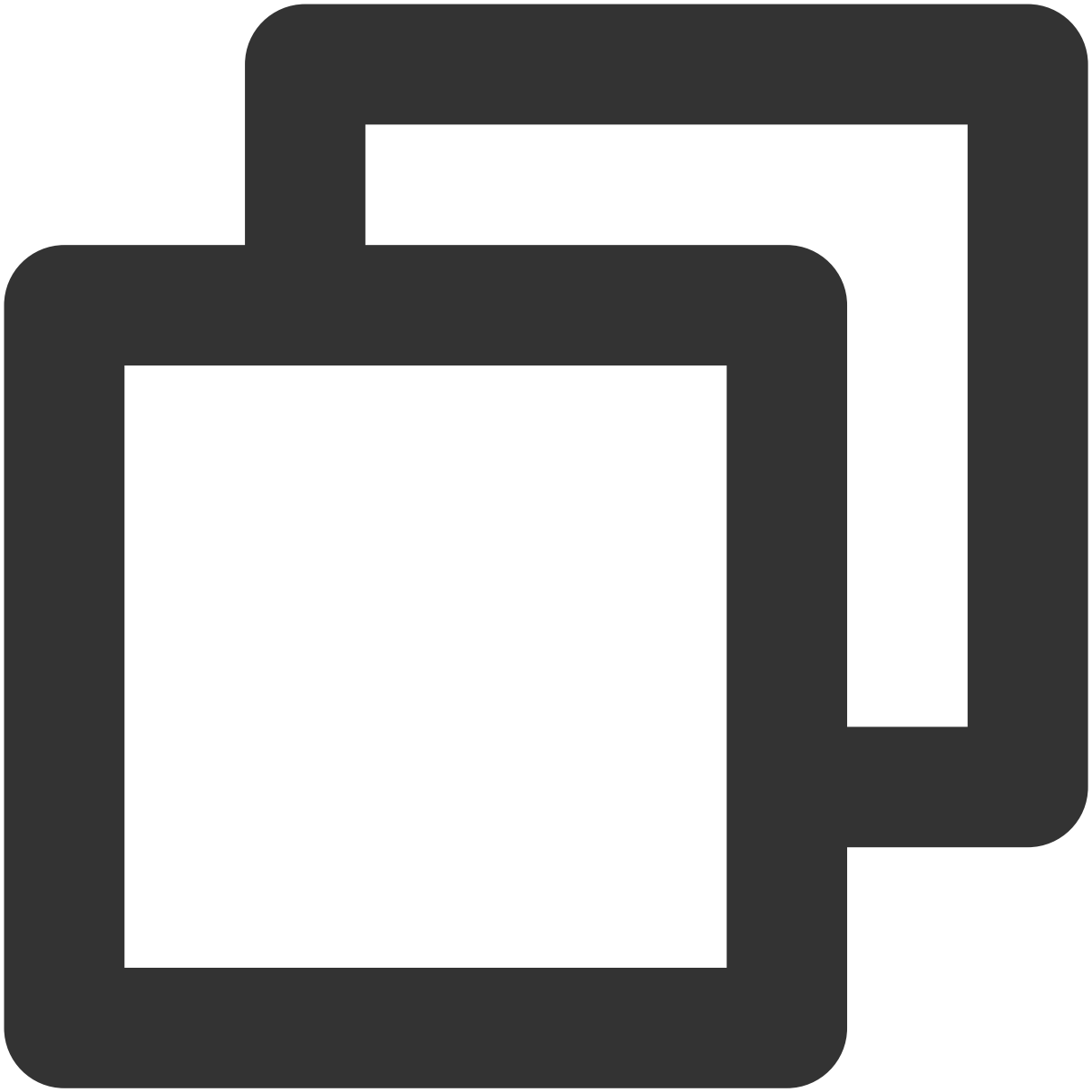
```
"action":["tpns:action1","tpns:action2"]
```

You can also specify multiple operations using a wildcard. For example, you can specify all operations whose names begin with "Describe" as shown below:



```
"action":["tpns:Describe*"]
```

To specify all Tencent Push Notification Service operations, use an asterisk (*) as follows:



```
"action"：["tpns:*"]
```

The following table describes the list of authorizable operations:

Note:

Only operations that support resource-level permissions can be authorized at the app level.

Operation	Description	Resource-Level Permission Supported
AddChannelInfo	Adds vendor-specific channel	Yes

CancelPush	Cancels scheduled push task	Yes
CreateApp	Creates app	No
CreateAppTrialRequest	Applies for product trial	Yes
CreateProduct	Creates product	No
DeleteAppInfo	Deletes app	Yes
DeleteProductInfo	Deletes product	No
DescribeApnsCertInfo	Queries APNS certificate information	Yes
DescribeAppAllTags	Queries all tag information	Yes
DescribeAppInfo	Queries app information	Yes
DescribeAppVipInfo	Queries VIP information	Yes
DescribeChannelInfo	Queries vendor-specific channel information	Yes
DescribeProductInfo	Queries product information	No
DescribeTagTokenNums	Queries the number of devices under the tag	Yes
DownloadPushPackage	Downloads push number package	Yes
DescribeAccountByToken	Queries account bound to device	Yes
DescribeAccountPushStatInfo	Queries the total number of push messages under account	No
DescribeAccountPushStatInfoAllZone	Queries the total number of messages supposed to be sent by all apps in cluster	No
DescribeAppSecretInfo	Queries `AppSecret` information	Yes
DescribeDeviceStatOverview	Queries the number of accumulated and daily active devices of app	Yes
DescribeProductDeviceStatWithRatioOverview	Queries app statistics	Yes
DescribePushPackaDescribeoken	Uploads number package to get	Yes

	temporary COS token	
DescribePushTaskGroupStatAllChannel	Queries the aggregated data of pushes in all channels	Yes
DescribePushTaskStatAllChannel	Queries the data of each push channel	Yes
DescribeTagsByToken	Queries tags bound to device	Yes
DescribeTokenInfos	Queries `tokenInfo` information	No
DescribePushInfos	Queries push list	Yes
ModifyAppInfo	Updates app information	Yes
ModifyProductInfo	Updates product information	No
CreatePush	Creates push	Yes
UpdateAppStatus	Updates app status	Yes
UploadCert	Uploads iOS certificate	Yes
UploadPushPackage	Uploads push number package	Yes
DescribePlanPushInfos	Queries the task list under the push plan	Yes
DescribePushPlans	Queries the list information about the push plan	Yes
UpdatePushPlan	Modifies a push plan	Yes
DeletePushPlan	Deletes a push plan	Yes
CreatePushPlan	Creates a push plan	Yes

Sample Policy for Operations Personnel

Suppose that the main responsibilities of the operations personnel are to view push records and create pushes. Then, the operation permissions can be queried according to the list of authorizable operations above:

All query operations

Canceling scheduled push tasks

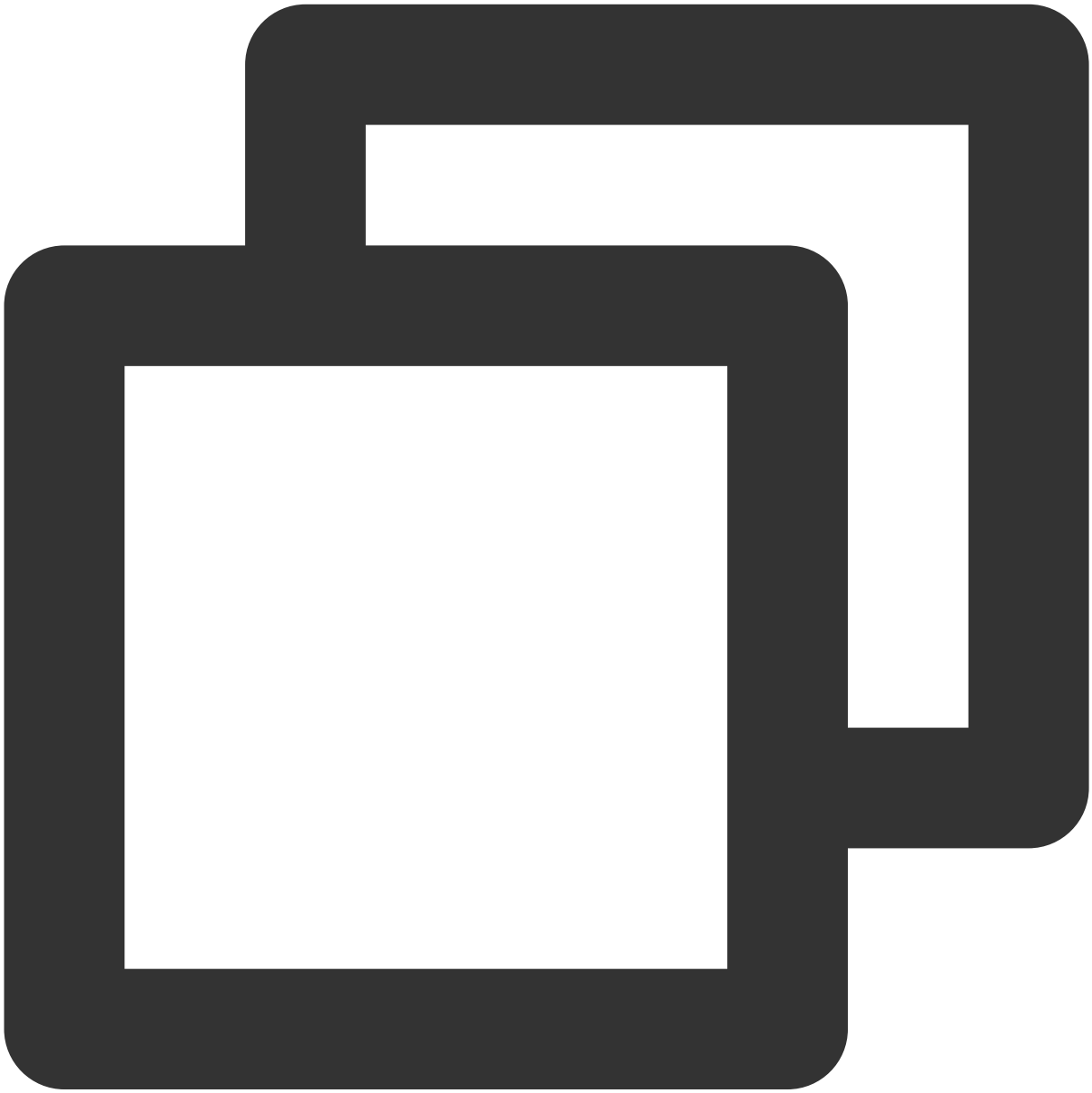
Creating pushes

Uploading push number packages

Downloading push number packages

Assume that the root account ID is `1000000000`, and the `Access_id` values of the authorized applications are `1500000000` and `1500000001`, respectively.

The corresponding policy syntax should be as follows:



```
//
{
    "version": "2.0",
    "statement": [
```

```
        {
            "action": [
                "tpns:Describe*",
                "tpns:CancelPush",
                "tpns:DownloadPushPackage",
                "tpns:CreatePush",
                "tpns:UploadPushPackage"
            ],
            "resource": [
                "qcs::tpns::uin/1000000000:app/1500000000","qcs::tpns::uin/10000000
            ],
            "effect": "allow"
        },
        {
            "action": [
                "tpns:Describe*"
            ],
            "resource": [
                "qcs::tpns::uin/1000000000:other/*"
            ],
            "effect": "allow"
        }

    ]
}
```

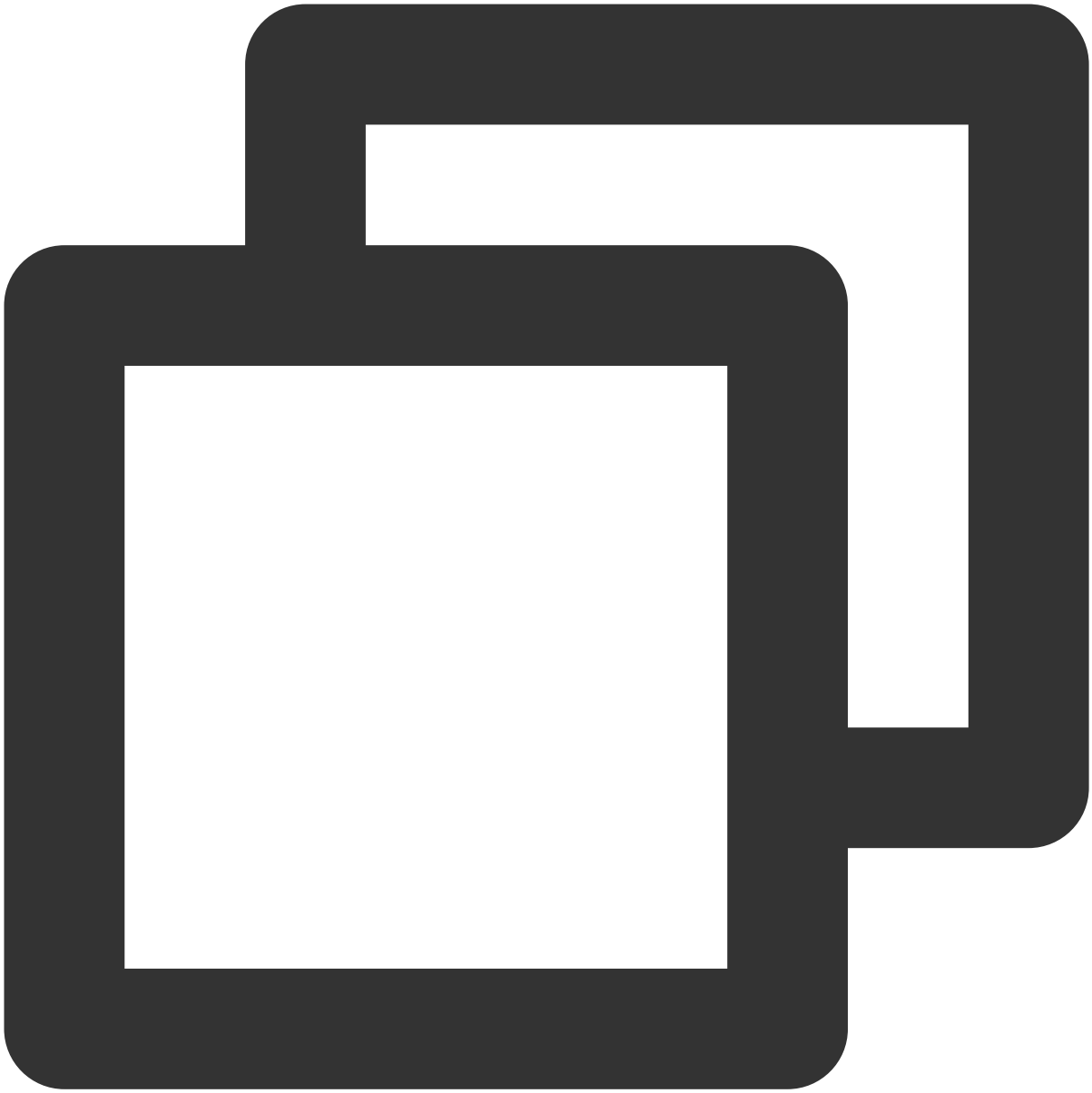
The created policy can be found at Policies in the CAM console. You can associate it with the sub-user to complete the permission configuration. Note that the policy can also be associated with other sub-users.

Sample Policy for Developers

Suppose that the main responsibilities of developers are to access and test. Then, all operation permissions should be granted.

Assume that the root account ID is `1000000000`, and the `Access_id` values of the authorized applications are `1500000000` and `1500000001`, respectively.

The corresponding policy syntax should be as follows:



```
//
{
    "version": "2.0",
    "statement": [
        {
            "action": "*",
            "resource": [
                "qcs::tpns::uin/1000000000:app/1500000000","qcs::tpns::uin/10000000
            ],
            "effect": "allow"
        },
```

```
        {
            "action": [
                "tpns:Describe*"
            ],
            "resource": [
                "qcs::tpns::uin/1000000000:other/*"
            ],
            "effect": "allow"
        }

    ]
}
```

The created policy can be found at Policies in the CAM console. You can associate it with the sub-user to complete the permission configuration. Note that the policy can also be associated with other sub-users.

Resource Tag

Last updated：2024-01-16 17:43:54

Resource tag is a resource management tool provided by Tencent Cloud. You can assign tags to Tencent Push Notification Service applications and then manage all applications under a certain resource tag in a unified way. Resource tag has the following two capabilities:

Cost allocation by tag

Authorization by tag

Resource tag divides into tag keys and tag values. One tag key can correspond to multiple tag values. You can authorize and allocate cost by tag in the following steps.

Use Cases

For example, if both the **application 1** and **application 2** created in Tencent Push Notification Service are owned by the **product department**, you can assign the tag `Department: Product Department` to both of them. Then, you can:

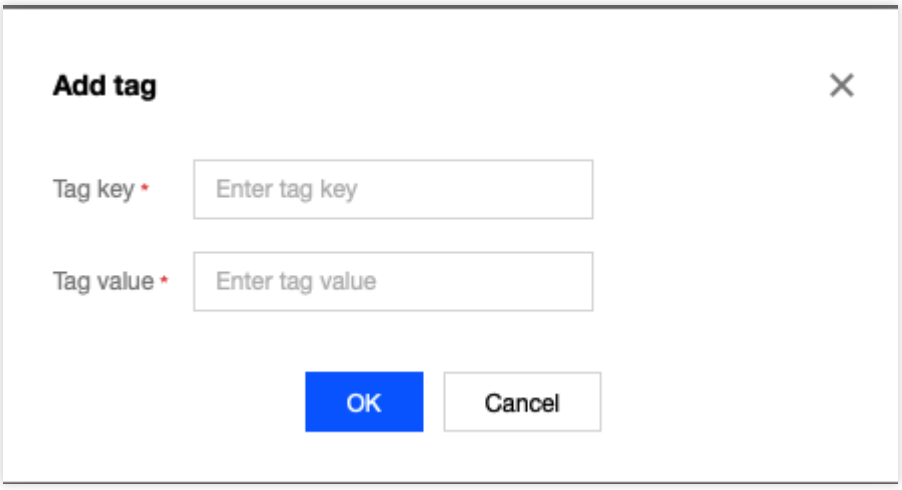
1. View the aggregated bill for all Tencent Cloud resources under the `Department: Product Department` tag, i.e., the total usage of the product department in Tencent Cloud.
2. Directly grant Tom (a new employee in the product department) permissions to manage all resources under the tag `Department: Product Departmen` .

The following describes how to use resource tags on the Tencent Push Notification Service platform:

Preparations

Step 1. Create a tag

1. Go to the Tag List page.
2. Click **Create** to access the tag creation page and enter the tag key and the corresponding tag value.



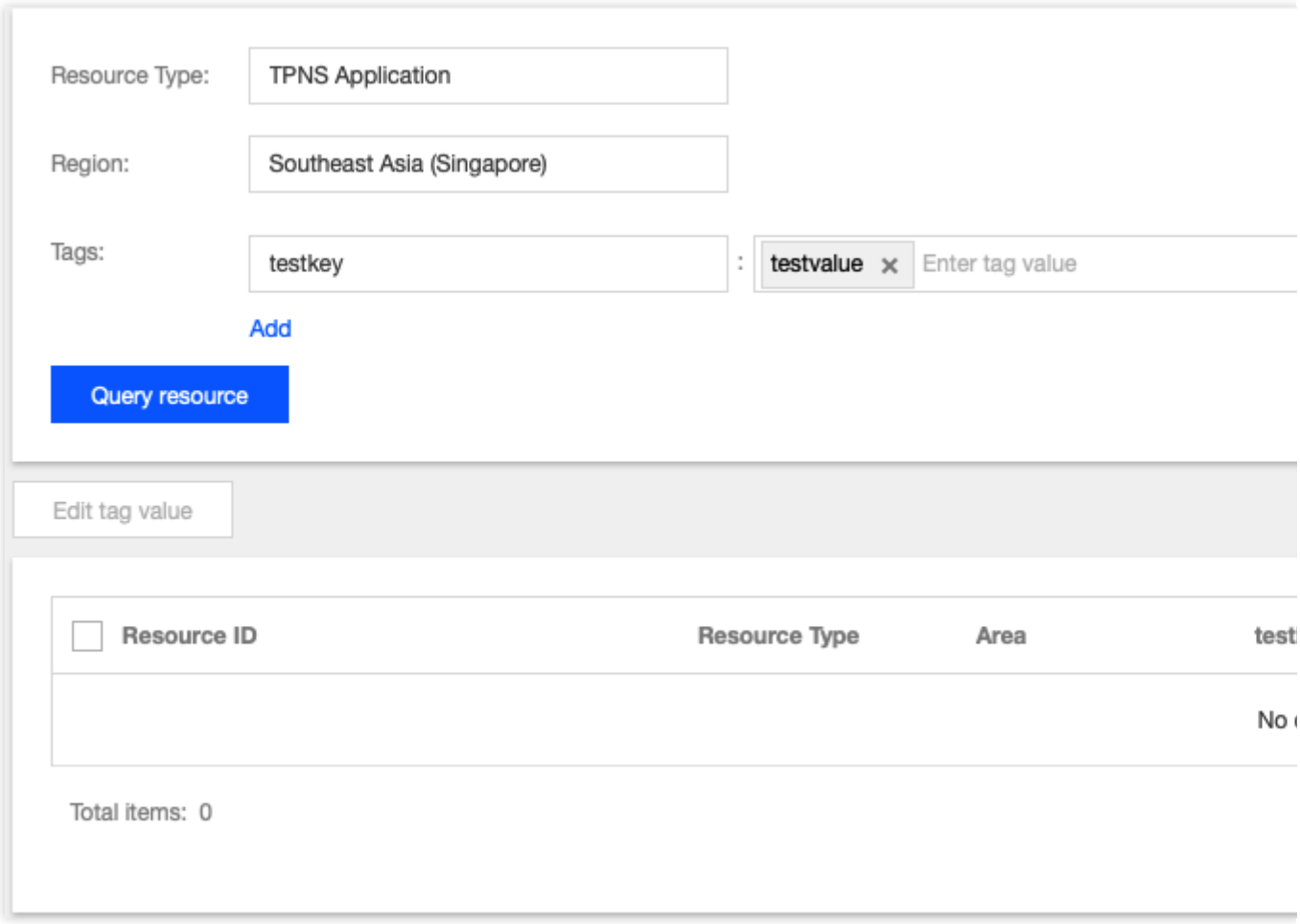
3. Click **OK**. You can view the creation result in the list at the bottom of the page.

Step 2. Assign tags to resources

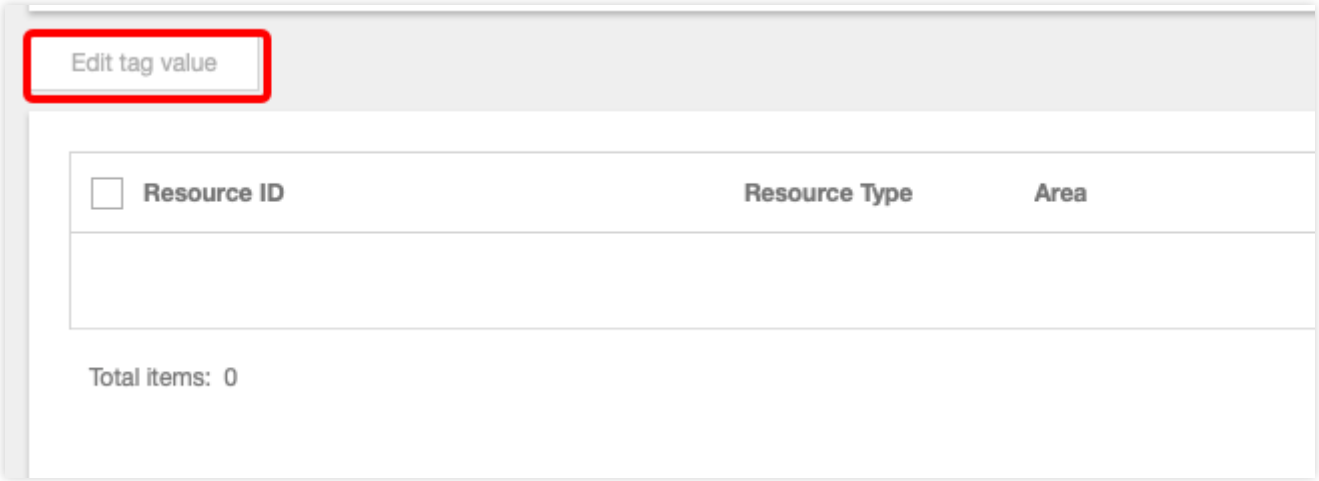
You can assign tags to Tencent Push Notification Service applications in the **Tag** or **Tencent Push Notification Service** console.

Tag console

1. After creating a tag, click **Resource Tag** on the left sidebar to enter the resource tag page.
2. You can enter the tag assignment page:
Resource Type: select "TPNS application".
Region: select the "service access point" you selected when creating the product in the Tencent Push Notification Service console.
3. After selecting **Resource Type** and **Region**, click **Query resource** to view all the applications you have created on the Tencent Push Notification Service platform. The **Resource ID** corresponds to the **AccessID** of a Tencent Push Notification Service application.



4. Select multiple applications in the list below and click **Edit tag value** above the list to assign the corresponding tag key-value pair to the selected applications.

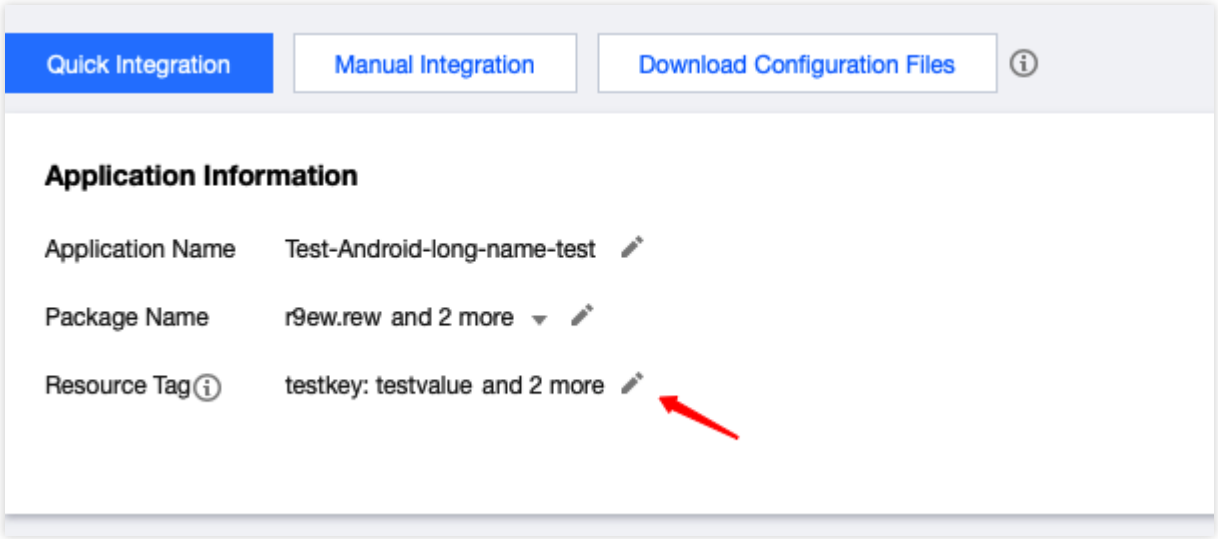


Tencent Push Notification Service console

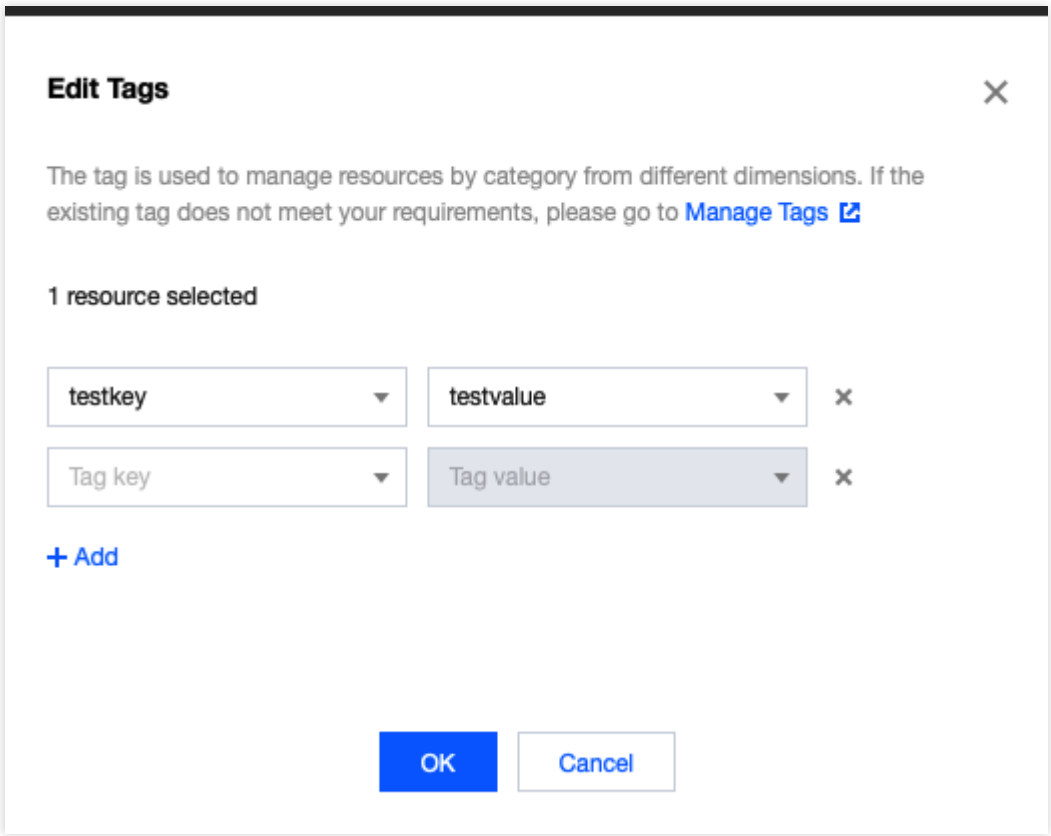
1. Log in to the Tencent Push Notification Service console, click **Configuration Management** > **Basic Configuration** on the left sidebar to view the basic configuration items of an application. (You can use the application

selector at the top of the page to select the application for which to assign a tag.)

2. Click the edit icon on the right of the **Tag** attribute in the **Application Information** block.



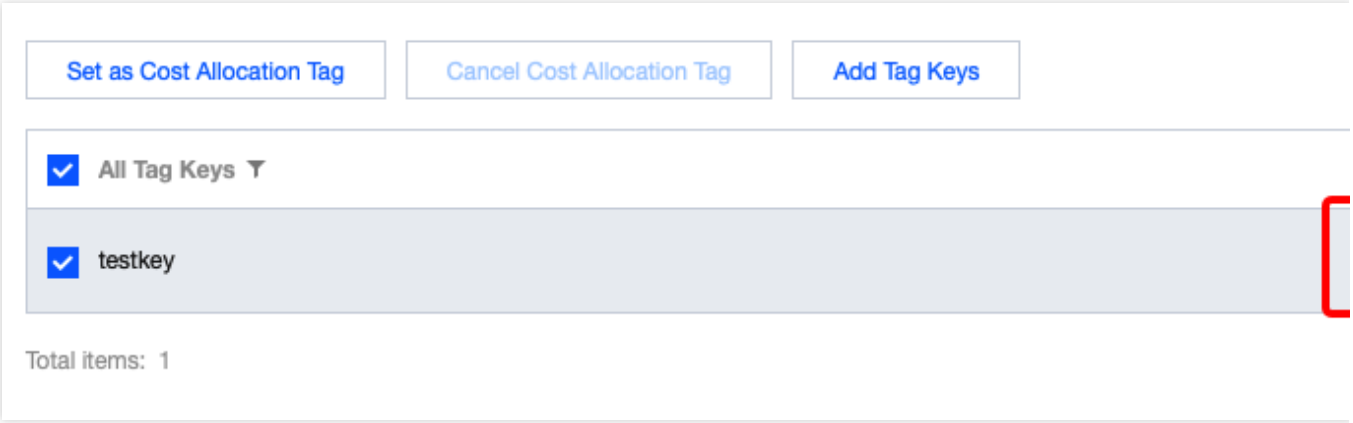
3. Then, the tag management module will pop up, where you can assign tags to the application.



Cost Allocation by Tag

Step 1. Set a cost allocation tag

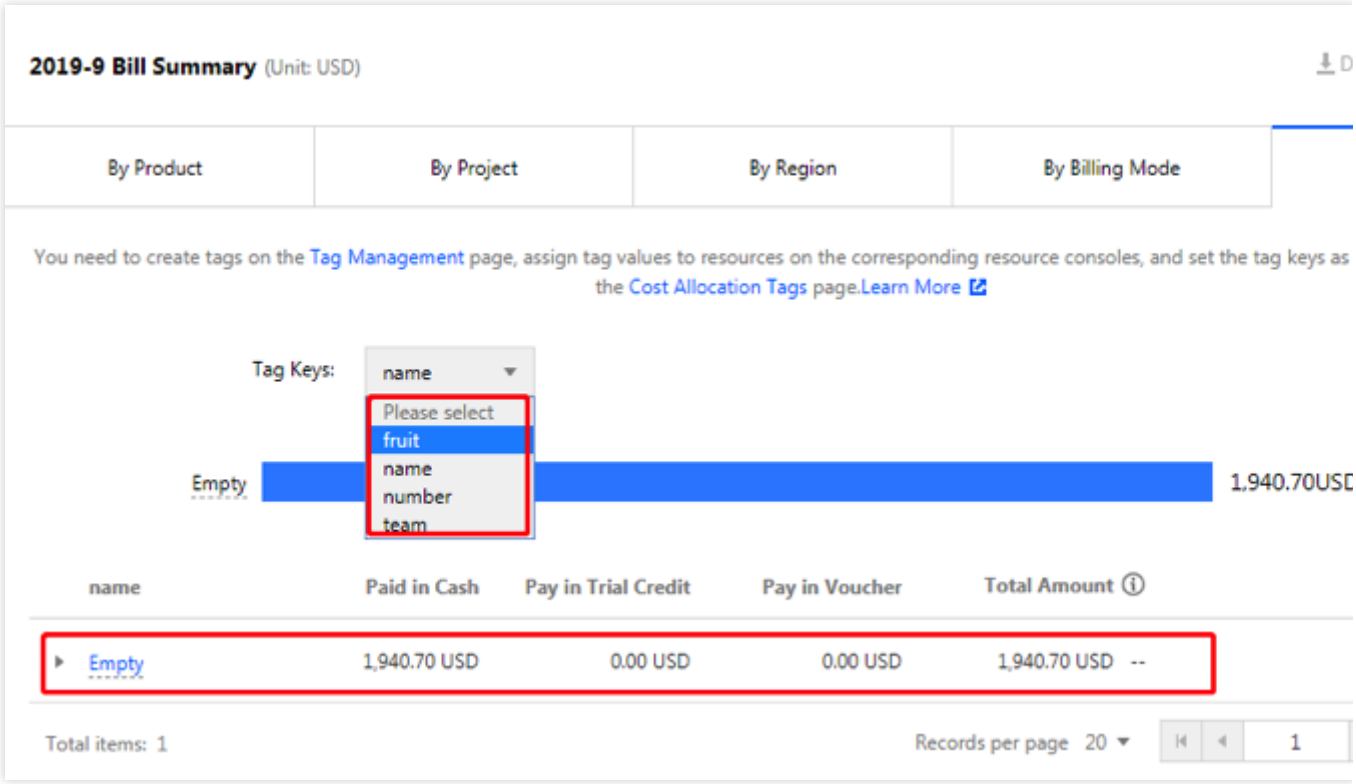
1. To use the tag feature for bills, you need to go to the Billing Center and select **Bills** > ** Cost Allocation Tags** on the left sidebar. The tag key set as a cost allocation tag will be displayed as a separate column of the bill. You can filter and categorize bills based on this tag key.
2. On this page, you can view the list of created tag keys. Select the tag key to be displayed and click **Set as Cost Allocation Tag** to set the tag key as a cost allocation tag in the bill.



Note:
You can set 5 cost allocation tags at most. We recommend that you select one tag key as the cost allocation tag, which makes it easier for you to manage your expenses.

Step 2. Display bills by tag

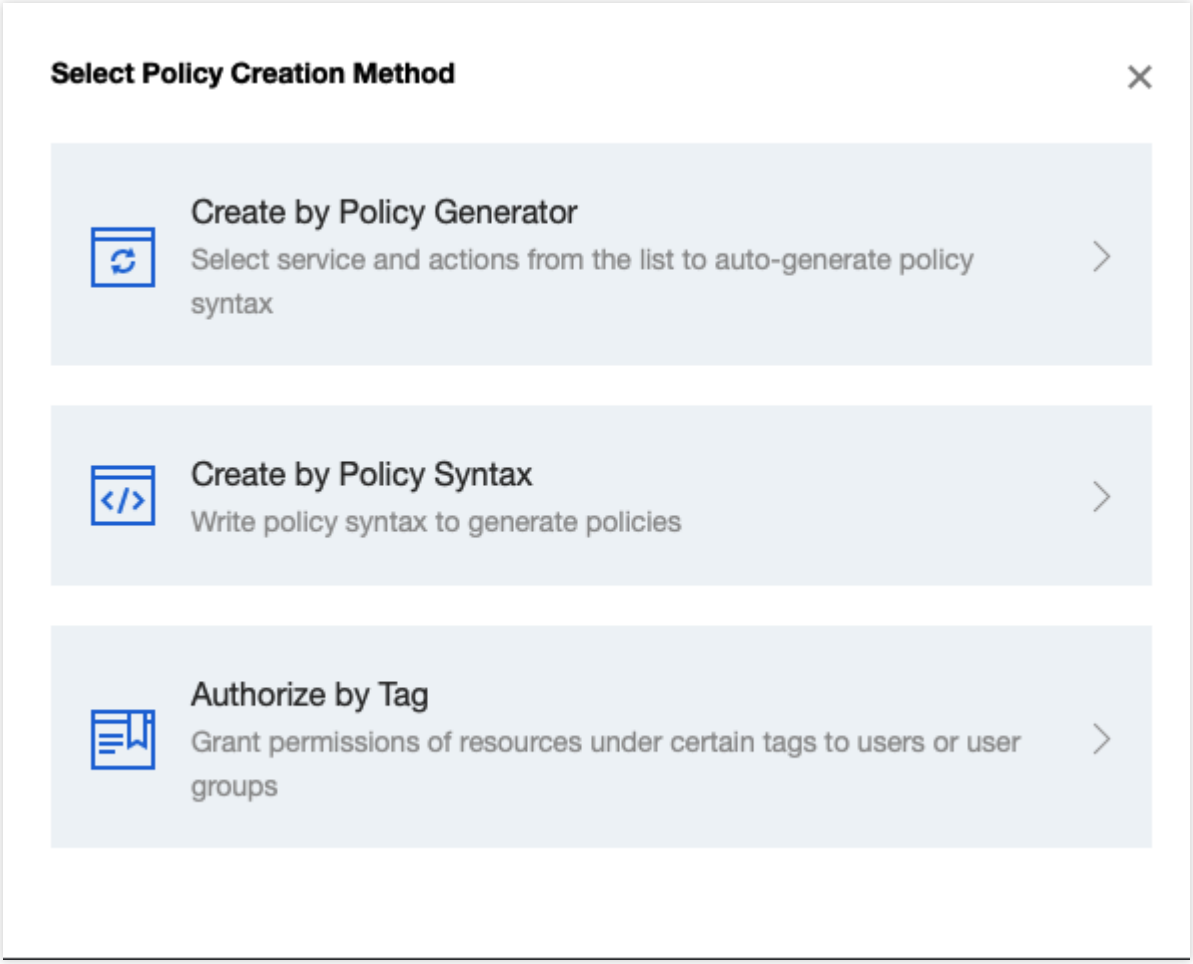
You can view and click the new option **By Tag** on the **Bill Overview** page. Then, you can select a specific **tag key** to view the histogram and list of relevant resources aggregated by the tag key.



Authorization by Tag

Authorization by tag means to quickly authorize resources under the same tag to a user or user group. The steps are as follows:

1. Go to the Policy page and click **Create Custom Policy** in the top-left corner.
2. In the creation method selection window that pops up, click **Authorize by Tag** to enter the "Authorize by Tag" page.



3. On the "Authorize by Tag" page, select the following information and click **Next** to enter the check page.

Authorized Users/User Groups: select the users/user groups to be authorized (choose one option).

Tag Keys: select the tag key to be authorized (required).

Tag Values: select the tag value to be authorized (required).

4. Click **Next**, check the policy (whose name can be customized), and click **Complete**.

At this point, you have completed authorization by tag. For more use cases of the tag feature, please see Product Overview.