

# **Tencent Push Notification Service**

# **Users and Permissions**

# **Product Documentation**





#### **Copyright Notice**

©2013-2024 Tencent Cloud. All rights reserved.

Copyright in this document is exclusively owned by Tencent Cloud. You must not reproduce, modify, copy or distribute in any way, in whole or in part, the contents of this document without Tencent Cloud's the prior written consent.

Trademark Notice

### 🔗 Tencent Cloud

All trademarks associated with Tencent Cloud and its services are owned by Tencent Cloud Computing (Beijing) Company Limited and its affiliated companies. Trademarks of third parties referred to in this document are owned by their respective proprietors.

#### Service Statement

This document is intended to provide users with general information about Tencent Cloud's products and services only and does not form part of Tencent Cloud's terms and conditions. Tencent Cloud's products or services are subject to change. Specific products and services and the standards applicable to them are exclusively provided for in Tencent Cloud's applicable terms and conditions.



## Contents

Users and Permissions

Quick Configuration

Advanced Custom Configuration

Resource Tag

# 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.

←	Create User
0	Click <u>Custom Greation</u> and select "Receive Messages Only" to create Message Recipients.
	R.
	Create one or more sub-users to grant your team access to your cloud resources.
	4° Guido Creation [2] Guiston Dreation
	Want to add an existing account as your mix-account?
	Create a Collaborator >

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

← Create Sub-user
1 User Type     >     ②     User Information     >     ③     User Permissions     >     ④     Review
User Type - Access Resources and Receive Messages The user will be able to log in to the console or use the API key to access the Tencent cloud resources within the scope of granted permissions, and have all the rights of a sub-account such as receiving messages.
Receive Messages Only
This user can only receive notifications from Tencent Cloud to your via mobile phone or email and cannot access Tencent Cloud.
Next

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.

← Create Sub-user						
Viser Type > 🗸 Viser	nformation > 3 User Permissions > 4 Review					
Select policies from the policy list	Use existing user policies Use group permissions					
Authorization Notes     If you want to grant the sub-accoun     If you want to grant access to all ret     If you want to grant read-only access	the full access permissions of all resources under the current account, select AdministratorAccess. surces except GAM and billing center under the current account to the sub-account, select QCioudResourceFullAccess. to all resources under the current account to the sub-account, select ReadOnlyAccess.					
Create Custom Policy 🗘 Policy List (2 total, 0 selected)						
Policy Name	Description	References				
QcloudTPNSFullAccess	Full read-write access to Tencent Push Notification Service (TPNS)	0				
QcloudTPNSReadOnlyAccess	Read-only access to Tencent Push Notification Service (TPNS)	0				
Support for holding shift key down for m	Itiple selection					
Self-service management of API keys ()	Self-service management of API keys () Self-service management of MFA devices ()					
Next	Next					

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.

← Create Sub-user	Create Sub-user				
✓ User Type > ✓ User Information > 3 User Permissions	> (4) Review				
Select policies from the policy list Use existing user policies Use group perm	issions				
Select policies from the policy list       Use existing user policies       Use group permissions         Image: Control of the sub-account of the sub-account to fine sub-account, select AdministratorAccess.       Image: Control of the sub-account to fine sub-account, select AdministratorAccess.         Image: Image: Image: Control of the sub-account to grant resources under the current account, select AdministratorAccess.       Image: Control of the sub-account, select AdministratorAccess.         Image: Image: Image: Control of the sub-account, select Resources under the current account, select ResourceFulAccess.       Image: Control of the sub-account, select ResourceSulAccess.					
Create Custom Policy Policy List (706 total, 0 selected)					
Create Sub-user     User Type     Vertige					
AdministratorAccess	This policy allows you to manage all users under your account and their permissions, financial info	1			
ReadOnlyAccess	This policy authorizes you with the read-only access to all cloud assets that support authenticatio	0			

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

Po	licies						
E							
			Service Type T				
				т	This policy allows you to manage all users under your account and their permission	ons, financial ir	formation and cloud assets.
				Select Po	olicy Creation Method	×	n at API or resource level in
			Application compliance platform	C	Create by Policy Generator Select service and actions from the list to auto-generate policy	>	
			Application compliance platform		Synax		
					Create by Policy Syntax		
			Alexam	(7)	Write policy syntax to generate policies		
			Al IoT Gateway		Authorize by Tag		
			Audio Moderation System	팯	Grant permissions of resources under certain tags to users or user groups	>	
			Anti-DDoS		8.eaha		

### 3. Select Blank Template.

← Create by Policy Syntax	
Select Policy Template > 2 Edit Policy	
Template Type: All Templates	
Select a template type	
All Templates (706 Total)	
O Blank Template	AdministratorAccess This policy allows you to manage all users under your account and their permissions, financial information and assets.
CloudFinanceFullAccess This policy allows you to manage all financial items in your account, such as payment and billing.	C QcloudACPFullAccess Full read-write access to ACP
C QcloudAdvisorFullAccess Full read-write access to Cloud Advisor (Advisor)	C QcloudAlexamFullAccess Full read-write access to Alexam
Next 2	

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

Select	Policy Template > 2	Edit Policy
Policy Name *	policygen-20220426161037	1
Description		
Policy Conte	nt Use Legacy Version	2
1 { 2 3 4	"version": "2.0", "statement": []	-
- 2		
Previous	Complete	

#### 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/150000000"
         1,
         "effect": "allow"
     },
     {
         "action":[
             "tpns:Describe*"
         ],
         "resource": [
             "qcs::tpns::uin/100000000:/*"
         ],
         "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.

					_
Account Center	Account Information				
2 Account Information		Basic Informati	ion		
Recurity Settings		Account Email	m	Verification Status	Ve
Project Management		Account Name	m 🌶	Industry	Ot
Identity		Account ID	100011279693	Contact Number	+8
Verification		APPID	1. 70	Contact Email	13
டி Message Subscription ம		Registered On			
		Modify			
		Full Name	Internet	City	Π
		Region	/e	Address	Π
		State	ппп	Postal Code	Π

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 150000000 in the syntax above with it. If you want to grant permissions of multiple applications, you can change resource to:



"qcs::tpns::uin/100000000:app/{Application Access\_ID

```
1}", "qcs::tpns::uin/100000000: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.

Create Sub-user							
✓ User Type > ✓ User Information > ③ User Permissions	> (4) Review						
Select policies from the policy list Use existing user policies Use group permis	sions						
Authorization Notes     If you want to grant the sub-account the full access permissions of all resources under the current     If you want to grant access to all resources except CAM and billing center under the current accounces     If you want to grant read-only access to all resources under the current to the sub-accounces	Authorization Notes     If you want to grant the sub-account the full access permissions of all resources under the current account, select AdministratorAccess.     If you want to grant access to all resources under the current account to the sub-account, select QCloudResourceFulAccess.     If you want to grant read-only access to all resources under the current account to the sub-account, select ReadOnlyAccess.						
Create Custom Policy 🗘 Policy List (706 total, 0 selected)							
Policy Name	Description	References					
AdministratorAccess	This policy allows you to manage all users under your account and their permissions, financial info	1					
ReadOnlyAccess	This policy authorizes you with the read-only access to all cloud assets that support authenticatio	0					

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 <code>effect</code> , <code>action</code> , <code>resource</code> , and <code>condition</code> . One policy has only one statement. An <code>action</code> (operation) describes an allowed or denied operation, which can be an API or a feature set (a set of specific APIs prefixed with <code>permid</code> ).
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:

Create Custom Policy Delete			
Policy Name	D	escription Se	ervice 1
AdministratorAccess	Th	is policy allows you to manage all users under your account and t	
QCloudResourceFullAccess	Select a r	method to create policy	
QCloudFinanceFullAccess		Create by policy generator	
QcloudNARMSFullAccess	C	Select services and operations from the list to automatically generate policy syntax	
QcloudNARMSReadOniyAccess		Serier and Portage	
QcloudAAFullAccess		Create by Policy Syntax	
QcloudAccessForAegisRole		Compile policy syntax to create related policy	
QcloudAccessForASRole		Authorize by tag	
QcloudAccessForBAASRole	町	Resources that have certain type of tag attribute are quickly authorized to users and user groups	
QcloudAccessForBKRole		annenzea te adore ana ador groupo	

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.

QcloudTPNSFullAcce Full read-write access to (TPNS)	ess Tencent Push Notification Service	0	QcloudTPNSReadOnlyAcc Read-only access to Tencent Pa
---	--	---	---

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/100000000: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 <code>name/tpns:</code> 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

STencent Cloud

	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

 $Assume that the root account ID is \verb| 100000000| and the \verb| Access_id| values of the authorized applications are \\ Access_id| values of the authoride applications are \\$ 

150000000 and 150000001 , 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/100000000:app/150000000", "qcs::tpns::uin/10000000
            ],
            "effect": "allow"
        },
        {
            "action": [
                "tpns:Describe*"
            ],
            "resource": [
                "qcs::tpns::uin/100000000: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 100000000, 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": [
            "resource": [
            "qcs::tpns::uin/10000000:app/150000000","qcs::tpns::uin/10000000
        ],
        "effect": "allow"
     },
```

```
{
    "action": [
    "tpns:Describe*"
    ],
    "resource": [
        "qcs::tpns::uin/100000000: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 Department.

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.

Add tag		×
Tag key *	Enter tag key	
Tag value *	Enter tag value	
	OK Cancel	

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.

Resource Type:	TPNS Application			
Region:	Southeast Asia (Singapore)			
Tags:	testkey	: testvalue ×	Enter tag value	
	Add			
Query resource	e			
Edit tag value				
Resource I	D	Resource Type	Area	test
				No
Total items: 0				

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.

C	Edit tag value		
	Resource ID	Resource Type	Area
	Total items: 0		
	Total items: 0		

### **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.

Quick Integration	Manual Integration	Download Configuration Files	<b>(i)</b>
Application Infor	mation		
Application Name	Test-Android-long-name-test	ľ	
Package Name	r9ew.rew and 2 more 👻 🎤		
Resource Tag(i)	testkey: testvalue and 2 more	e /*	

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

e resource			
et your req	es by category from differ uirements, please go to N	ent dimens Manage Tag	sions. If the gs 🖸
•	testvalue	*	×
•	Tag value	Ψ.	×
	OK Cancel		
	•	<ul> <li>▼ testvalue</li> <li>▼ Tag value</li> <li>OK Cancel</li> </ul>	<ul> <li>▼ testvalue</li> <li>▼ Tag value</li> <li>▼ OK Cancel</li> </ul>

## 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.

Set as Cost Allocation Tag	Cancel Cost Allocation Tag	Add Tag Keys
All Tag Keys ¥		
testkey		

### 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.

	By Projec	ct	By Region	By Billing Mode	
u need to create tags on the Ta	ag Management pag	e, assign tag values to re: the Cost Alloca	ources on the correspon	ding resource consoles, and s	set the tag keys
Tao Kee					
lag Key	Please select				
Empty	name number				1,940.70U
	team				
name	Paid in Cash	Pay in Trial Credit	Pay in Voucher	Total Amount 🛈	

# 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.

:	Select Po	licy Creation Method	×
	C	Create by Policy Generator Select service and actions from the list to auto-generate policy syntax	>
		Create by Policy Syntax Write policy syntax to generate policies	>
	III	Authorize by Tag Grant permissions of resources under certain tags to users or user groups	>

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.