ALIBABA CLOUD

Alibaba Cloud

API Gateway

Quick Start

Document Version: 20220311

Alibaba Cloud

Legal disclaimer

Alibaba Cloud reminds you to carefully read and fully understand the terms and conditions of this legal disclaimer before you read or use this document. If you have read or used this document, it shall be deemed as your total acceptance of this legal disclaimer.

1. You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.

2. No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company or individual in any form or by any means without the prior written consent of Alibaba Cloud.

3. The content of this document may be changed because of product version upgrade, adjustment, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and an updated version of this document will be released through Alibaba Cloud-authorized channels from time to time. You should pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.

4. This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides this document based on the "status quo", "being defective", and "existing functions" of its products and services. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity, applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not take legal responsibility for any errors or lost profits incurred by any organization, company, or individual arising from download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, take responsibility for any indirect, consequential, punitive, contingent, special, or punitive damages, including lost profits arising from the use or trust in this document (even if Alibaba Cloud has been notified of the possibility of such a loss).

5. By law, all the contents in Alibaba Cloud documents, including but not limited to pictures, architecture design, page layout, and text description, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of this document shall be used, modified, reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates. The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates.

6. Please directly contact Alibaba Cloud for any errors of this document.

Document conventions

Style	Description	Example
Danger	A danger notice indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	**Danger:** Resetting will result in the loss of user configuration data.
Warning	A warning notice indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	**Warning:** Restarting will cause business interruption. About 10 minutes are required to restart an instance.
Notice	A caution notice indicates warning information, supplementary instructions, and other content that the user must understand.	**Notice:** If the weight is set to 0, the server no longer receives new requests.
Note	A note indicates supplemental instructions, best practices, tips, and other content.	**Note:** You can use Ctrl + A to select all files.
>	Closing angle brackets are used to indicate a multi-level menu cascade.	Click **Settings**> **Network**> **Set network type**.
Bold	Bold formatting is used for buttons , menus, page names, and other UI elements.	Click **OK**.
`Courier font`	Courier font is used for commands	Run the `cd /d C:/window` command to enter the Windows system folder.
Italic	Italic formatting is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	This format is used for an optional value, where only one item can be selected.	`ipconfig [-all|-t]`
{} or {a|b}	This format is used for a required value, where only one item can be selected.	`switch {active|stand}`

Table of Contents

1.Use a backend service to create and manage APIs

This topic describes how to create a backend service in the API Gateway console. This topic also describes how to use the created backend service to create, publish, and manage APIs.

Overview

To help you efficiently manage a growing number of APIs, API Gateway abstracts backend services as resources in regions. In the API Gateway console, you can create a backend service and define different URLs for the backend service in different environments. Then, you can select the backend service when you create an API that uses the backend service. This way, requests to call the API are routed to the corresponding URL of the backend service based on the environment to which the API is published. You can also manage all the published APIs that use a backend service in a centralized manner on the page for configuring the backend service. For example, the following scenarios are supported:

Scenario 1: After you change the URL of a backend service in the test environment, all the published APIs that use the backend service in the test environment are automatically updated without requiring you to republish the APIs. Requests to call the APIs are then routed to the new URL of the backend service in the test environment.

Scenario 2: After you delete the URL that is no longer needed for a backend service in the test environment, all the published APIs that use the backend service in the test environment are unpublished.

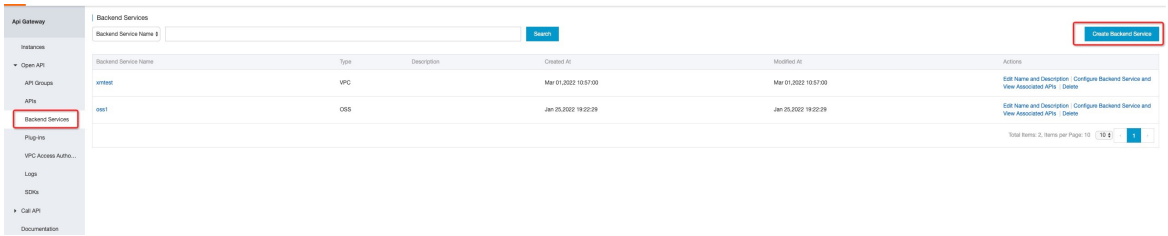
For more information, see the following text.

Procedure

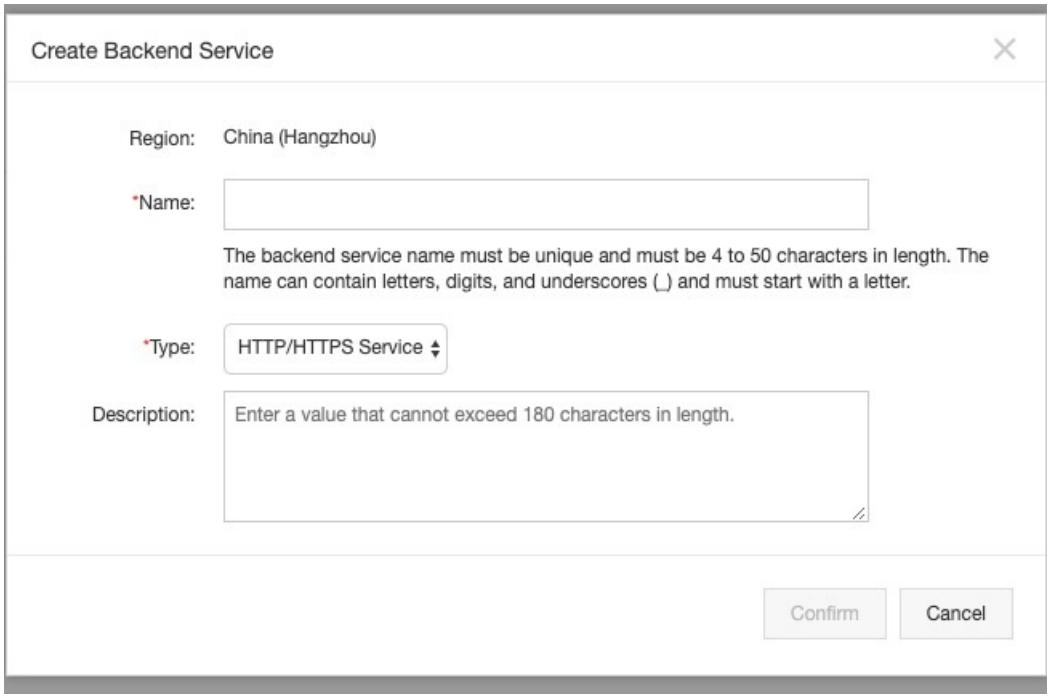
1. Create a backend service.
2. Define different URLs for the backend service in different environments.
3. Create and define an API.
4. Create an app and grant the app the permissions to call the API.
5. Debug the API.
6. Manage all the published APIs that use the backend service in a specific environment.

Create a backend service

1. Log on to the API Gateway console. In the left-side navigation pane, choose Open API > Backend Services. The Backend Services page appears.



2. Click Create Backend Service in the upper-right corner of the page. In the Create Backend Service dialog box, create a backend service. In this example, the Type parameter is set to HTTP/HTTPS Service.

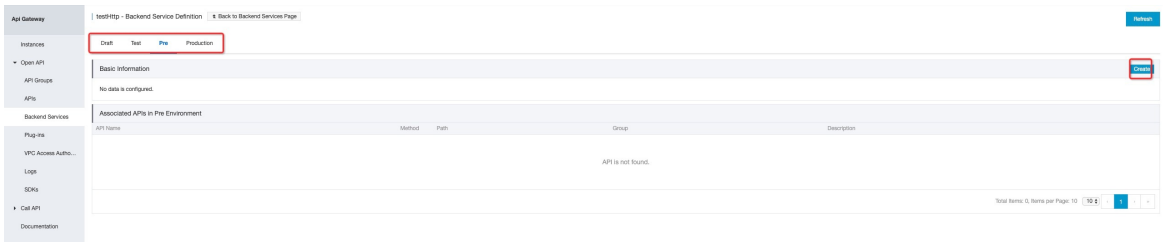


You must specify a type for each backend service, as shown in the preceding figure. After a backend service is created, you cannot change its type. However, you can change the name and description of the backend service as required. The valid values of the Type parameter are HTTP/HTTPS Service, VPC, Function Compute, OSS, and MOCK.

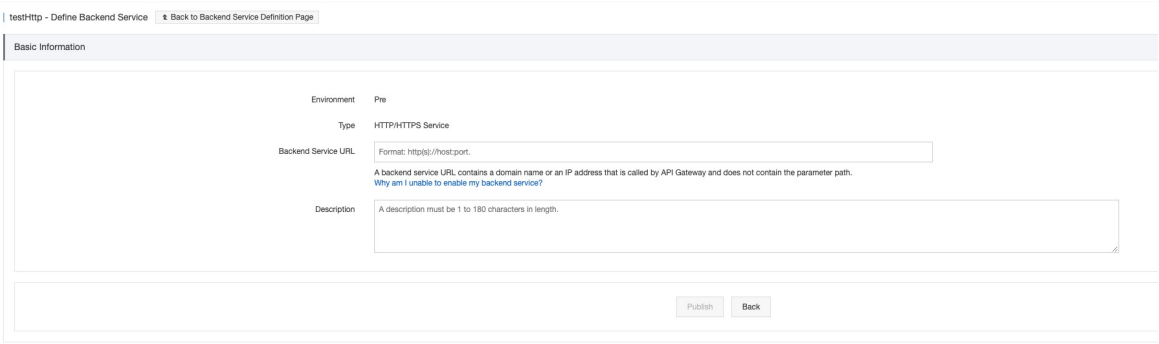
> **Notice**
>
> API Gateway of the current version does not support Object Storage Service (OSS) as the backend service on Finance Cloud or Alibaba Gov Cloud. API Gateway of future versions will allow you to create APIs that use OSS as the backend service on Finance Cloud and Alibaba Gov Cloud.

Define different URLs for the backend service in different environments

1. Find the backend service that you created and click Configure Backend Service and View Associated APIs in the Actions column. The Backend Service Definition page appears.The page contains four tabs, as shown in the preceding figure. On the Draft tab, you can view all the APIs that use the backend service. On each of the Test, Pre, and Production tabs, you can define a URL for the backend service and view all the published APIs that use the backend service.



2. Click one of the Test, Pre, and Production tabs. In this example, click the Test tab. Click Create in the upper-right corner.On the Define Backend Service page, enter a URL for the backend service and click Publish, as shown in the preceding figure. The Published message appears. Then, you can create an API.



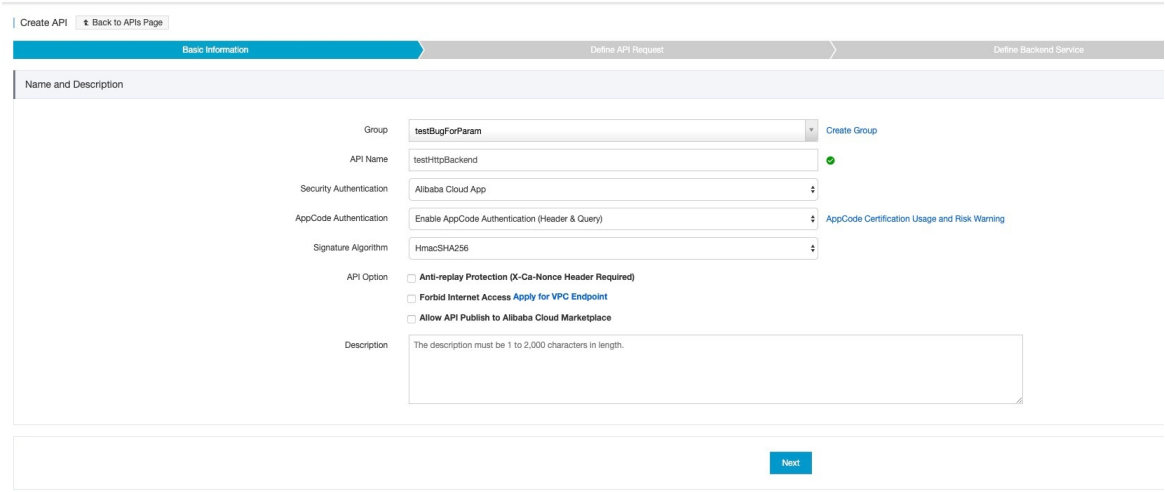
3. Take note of the following description when you define URLs for different types of backend services.

> **Note**
>
> If you use an HTTP or HTTPS backend service, you need only to enter the URL of the backend service.
>
> If you use a resource in a virtual private cloud (VPC) as the backend service, you must select an authorization rule that you create when you authorize API Gateway to access the VPC. Select Use HTTPS as required. If you select Use HTTPS, the HTTPS protocol is used to request the backend service.
>
> If you use Function Compute as the backend service, you must specify whether to select Event Function or HTTP Function for the Function Type parameter. If you select Event Function, configure the parameters as required. If you select HTTP Function, specify a trigger path.
>
> If you use OSS as the backend service, you must authorize API Gateway to access objects in your OSS bucket. To grant the read permissions to API Gateway, allow API Gateway to perform the oss:GetObject operation on the OSS bucket. To grant the write permissions to API Gateway, allow API Gateway to perform the oss:PutObject and oss:DeleteObject operations on the OSS bucket. To revoke the permissions granted to API Gateway, you can manually delete the relevant authorization policies from the OSS bucket.

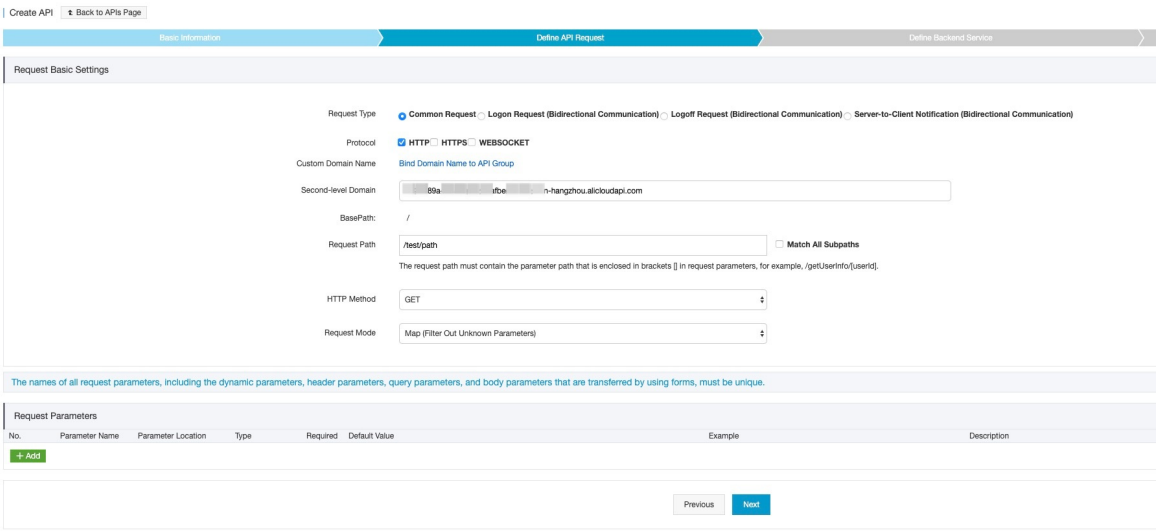
Create and define an API

1. In the left-side navigation pane, choose Open API > APIs. On the APIs page, click Create API in the upper-right corner. The Create API page appears.

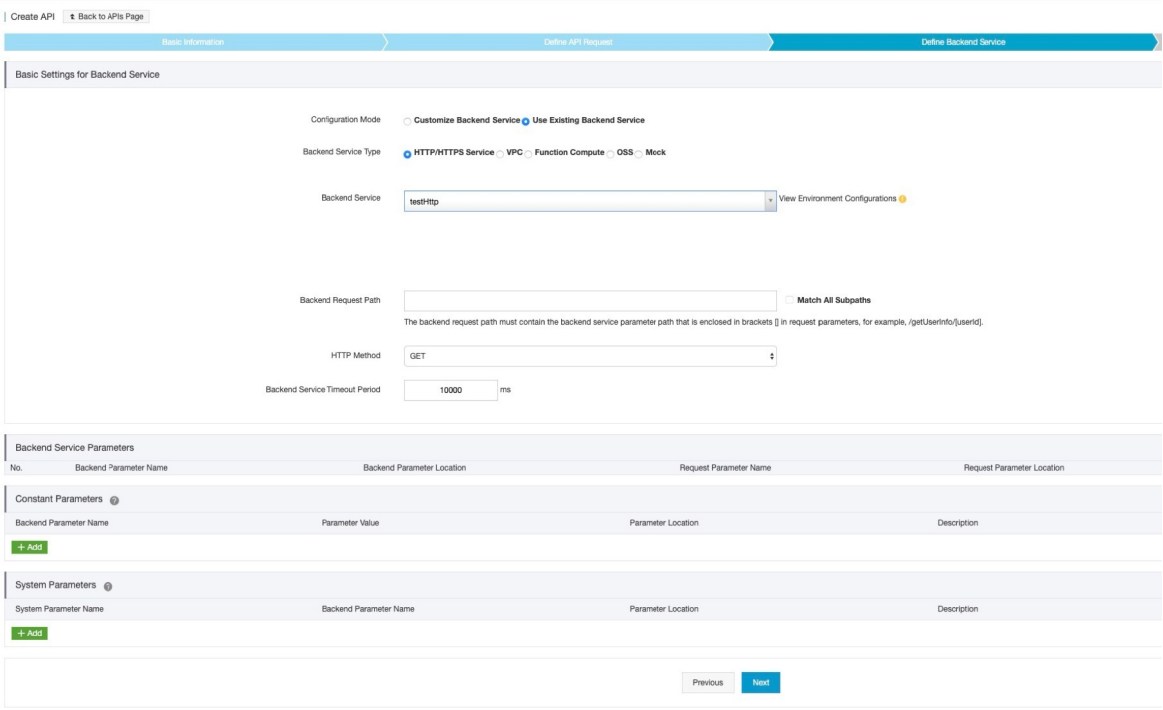
2. In the Basic Information step, configure the basic information about the API to be created, including the group to which the API belongs and the name, authentication method, type, and description of the API. Select a group, configure the other parameters, and then click Next. To facilitate subsequent testing, set the AppCode Authentication parameter to **Enable AppCode Authentication (Header & Query)**.



3. In the Define API Request step, define how a client, such as a browser, a mobile app, or a business system, sends a request for the API. Configure the Request Type, Protocol, Request Path, HTTP Method, and Request Mode parameters and add parameters in the Request Parameters section. Then, click Next. In this example, set the HTTP Method parameter to GET and the Request Mode parameter to Pass-through. A value of Pass-through indicates that API Gateway passes the received parameters to the backend service without processing.



4. In the Define Backend Service step, configure the type and URL of the backend service to which API Gateway sends the requests received from a client and how parameters are mapped and processed. The following example describes how to use an existing backend service.Select Use Existing Backend Service for the Configuration Mode parameter and HTTP/HTTPS Service for the Backend Service Type parameter. The console automatically searches for backend services of the selected type. Select the testHttp backend service that you create from the Backend Service drop-down list. To view the URLs of the backend service in different environments, move the pointer over View Environment Configurations and click the corresponding tabs. After you select a backend service, configure the other parameters that appear based on the type of the backend service. To create an API that uses an HTTP or HTTPS backend service, you must set the Backend Request Path, HTTP Method, and Backend Service Timeout Period parameters.



5. In the Define Response step, configure response information to generate API documentation. The documentation helps API callers better understand the API. You can configure the Response ContentType, Response Example, and Error Response Example parameters. In this example, this step is skipped. Click Create.

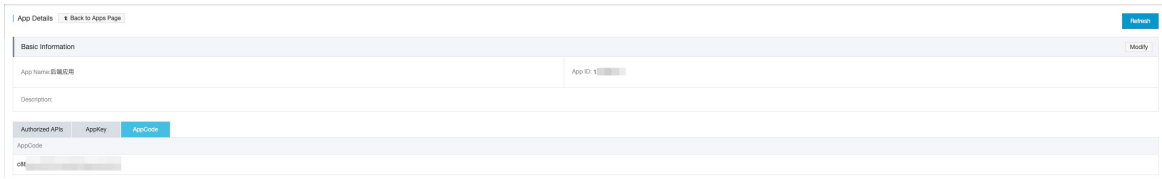
6. After you click Create, a message appears to inform you to publish the API. API Gateway provides three environments to which you can publish an API: Production, Pre, and Test. All configurations that you perform on an API can take effect only after you publish the API to a required environment.

> **Notice**
>
> Before you publish an API that uses a backend service to an environment, make sure that the backend service is defined in the environment. Otherwise, you cannot publish the API.

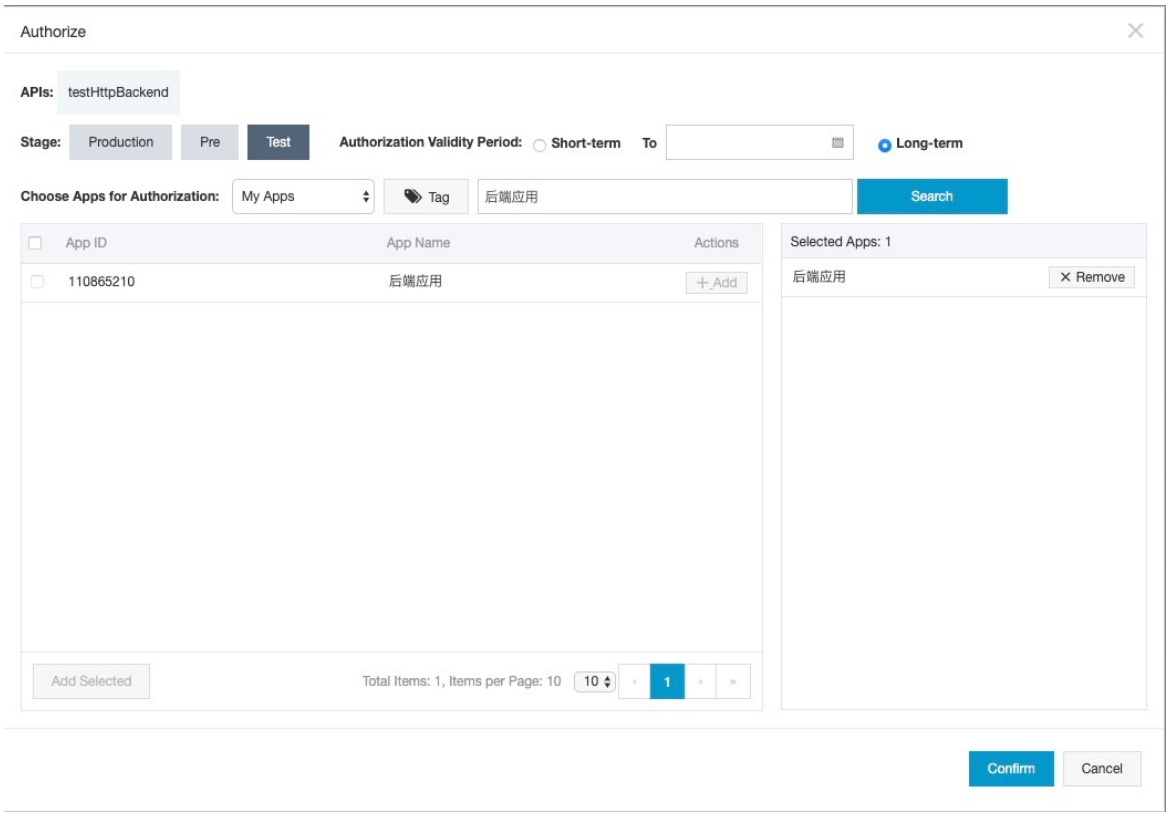
Create an app and grant the app the permissions to call the API

1. An app is an identity that you use to call the API. In the preceding step for creating the API, the Security Authentication parameter is set to Alibaba Cloud App. After you publish the API, you must create an app and grant the app the permissions to call the API.

2. In the left-side navigation pane, choose Call API > Apps. On the Apps page, click Create App in the upper-right corner. In the Create App dialog box, enter an app name and click Confirm. In the app list, click the name of the created app. The App Details page appears, as shown in the following figure. Two authentication modes are provided for the security authentication method Alibaba Cloud App: an AppKey and AppSecret pair and AppCode. In this example, the AppCode mode is used to authenticate the app. For more information about the security authentication method Alibaba Cloud App, see Call an API operation by using an AppCode.



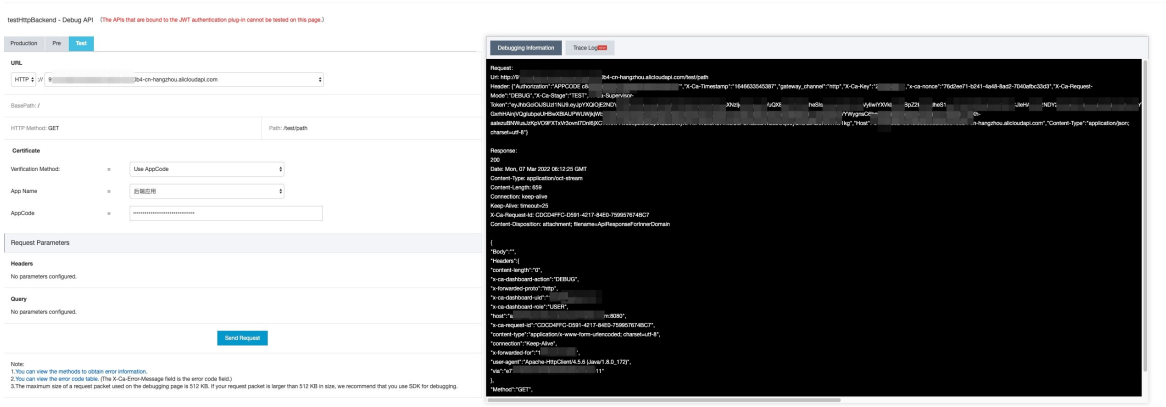
3. In the left-side navigation pane, choose Open API > APIs. On the APIs page, find the created API and choose More > Authorize in the Actions column. The Authorize dialog box appears, as shown in the following figure. Set the Stage parameter to the environment to which you publish the API. Enter the name of the app that you created in the search bar of the Choose Apps for Authorization section. In the search result, select the created app, click Add in the Actions column, and then click Confirm. A message appears to inform you that the app is authorized to call the API.



Debug the API

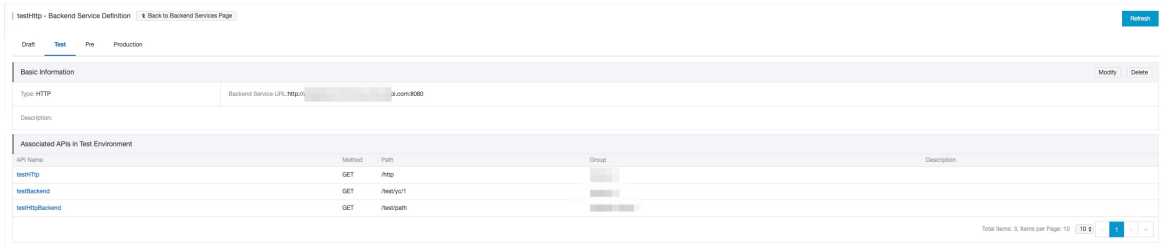
Debug the API after the authorization is successful. API Gateway supports online debugging. We recommend that you use this feature to check whether an API is correctly configured before you call the API on a client. On the APIs page, click the name of the created API. On the API details page, click Debug API in the left-side navigation pane. The following figure shows the page that appears. If you have defined request parameters for the API, you can enter different values for the request parameters to check whether the API is correctly configured. When you debug the API, make sure that the App Name parameter is set to the authorized app. The environment for debugging must be the one in which the app is authorized to call the API. Otherwise, the debugging may fail.

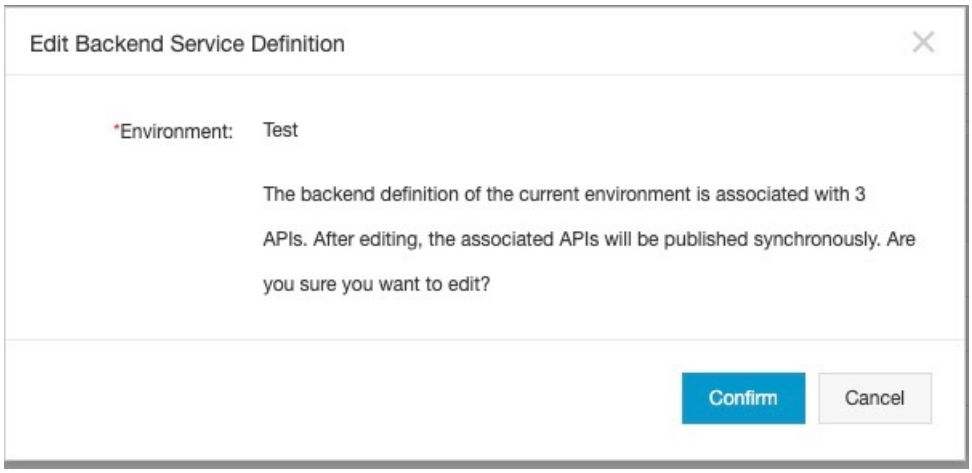
1.



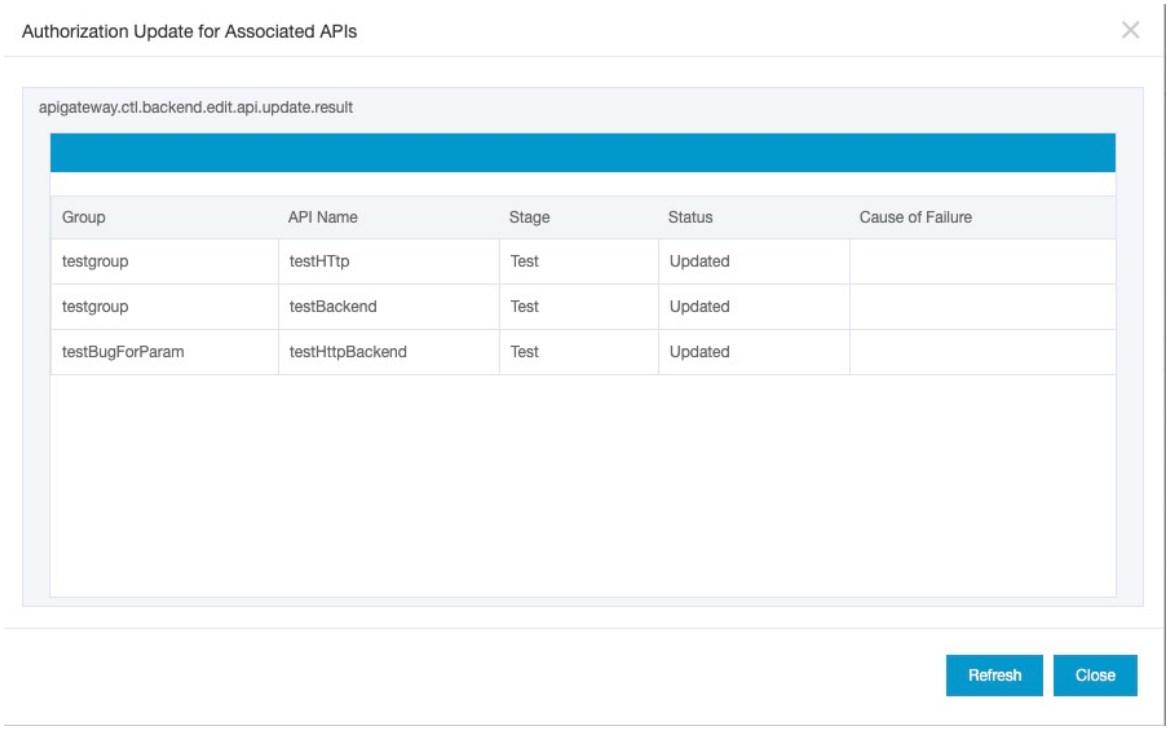
Manage all the published APIs that use the backend service in a specific environment

1. If you modify the definition of the backend service in a specific environment, all the published APIs that use the backend service in the environment are automatically updated. The following figure shows an example.Multiple APIs that use the testHttp backend service are published to the test environment, as shown in the preceding figure. Click Modify in the upper-right corner of the Basic Information section. On the Define Backend Service page, change the backend service URL and click Publish. A message appears to inform you that the backend service URL will be updated for all the published APIs that use the backend service in the test environment.

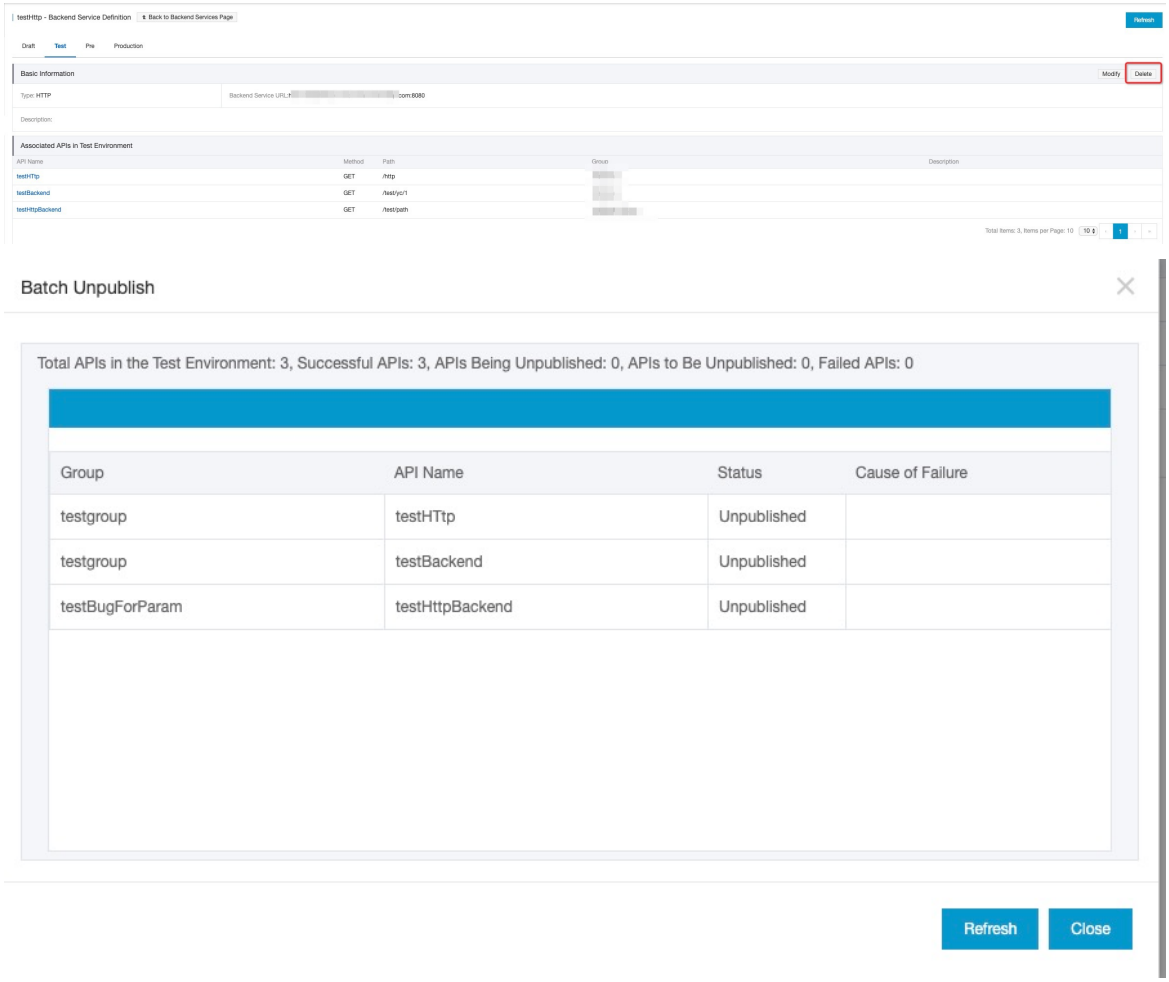




After you confirm to modify the definition of the backend service, you can see that the published APIs in the API list are updated. When you send requests to call the APIs again, the requests are routed to the new backend service URL.



2. If the backend service URL that you define for a specific environment is no longer needed, you can delete the definition of the backend service in the environment.If you delete the definition of the backend service in the environment, all the published APIs that use the backend service in the environment are unpublished. The following figure shows an example.



Warning

The preceding operations are performed on all associated APIs and are irreversible. Proceed with caution.

2.Create an API with OSS as the backend service

This topic describes how to create and publish an API with Object Storage Service (OSS) as the backend service in API Gateway, and how to call the API by using an AppKey and AppSecret pair of an APP. The AppKey and AppSecret are automatically generated for the APP if you set the authentication method of the API to Alibaba Cloud APP.

1. Overview

You must perform the following steps in sequence:

- Activate OSS
- Create an API group
- Create and define an API
- Create an APP and grant the APP the permissions to call the API
-
- Debug the API
- Call the API

2. Create an OSS bucket

OSS is a secure and cost-effective Alibaba Cloud service that allows you to store a large amount of data with high persistence. OSS provides console-independent RESTful API operations for you to store and access data of any type anytime, anywhere, and from any application. API Gateway supports creating an API whose backend service is OSS. When you create an API with OSS as the backend service to perform operations on OSS. You can not only upload objects to, download objects from, and delete objects from your buckets, but also integrate the capabilities of API Gateway to provide more reliable services for your business. In addition, if you activate API Gateway and OSS in the same region, APIs can access OSS over the internal network.

Step 1 Activate OSS

Log on to the Alibaba Cloud console, search for OSS, and then follow the instructions to activate OSS.

Step 2: Create an OSS bucket

For more information about how to create an OSS bucket, see OSS documentation. In this example, set the parameters as required, as shown in the following figure.

3. Create an API group

APIs are managed in API groups. Before you create an API, you must create an API group.

Step 3: Create an API group

In the left-side navigation pane, choose `Open API` > `Groups`. In the top navigation bar, select the region where you want to create an API group. On the API Groups page, click Create Group. In the Create Group dialog box, select your dedicated instance and set the Group Name parameter to testOssGroup. Only dedicated instances of a specific version and later support APIs with OSS as the backend service. If your dedicated instance is of an earlier version, contact Alibaba Cloud technical support to upgrade your instance.

Step 4: View the details of the API group

After you create the API group, the API group appears on the API Groups page. You can click the group name to go to the Group Details page. On this page, you can bind a domain name, modify basic information, and change the instance type.

After an API group is created, API Gateway automatically creates a public second-level domain for the API group. This default second-level domain can be used only to test API calls and can be used for a maximum of 1,000 times per day. We recommend that you bind an independent domain name after you create an API group. In this example, the default second-level domain is used.

4. Create an API

In the left-side navigation pane, choose `Open APIs` > `APIs`. Make sure that the current region is the same region where the API group you created resides. On the APIs page, click Create API.

Step 5: Configure basic information for the API

In this step, configure the basic information for the API to be created, including the API group to which the API belongs and the name, authentication method, type, and description of the API. In this example, set the Group parameter to the API group you created and the AppCode Authentication parameter to **Enable AppCode Authentication (Header & Query)**. Set other parameters as required and click Next.

Step 6: Configure request information for the API

In this step, define how a client, such as a browser, a mobile app, or a business system, sends a request for the API. The parameters that need to be specified in this step include Request Type, Protocol, Request Path, HTTP Method, Request Mode, and the parameters in the Request Parameters section. Then, click Next. In this example, set the HTTP Method parameter to **GET**, the Request Mode parameter to **Pass-through**. A value of Pass-through indicates that API Gateway passes the received parameters to the backend service without processing.

> **Note**
>
> Note that the HTTP method that you specify for the API determines the available API operations of OSS. API Gateway supports the GET, PUT, POST, HEAD, and DELETE methods for APIs that use OSS as the backend service. The methods support the following API operations of OSS:
>
> GET: GetObject
>
> PUT: PutObject
>
> POST: PostObject and AppendObject
>
> HEAD: HeadObject and GetObjectMeta
>
> DELETE and DeleteObject
>
> For more information about the description of the API operations, see API Reference of OSS.

Step 7: Configure backend service information for the API

In this step, configure a backend service type and a backend service address of the API and the mappings between request and response parameters. In this example, set the Backend Service Type parameter to OSS. Set the Action parameter to GetObject because GET is specified as the request method in the preceding step. We recommend that you select the region where both OSS and API Gateway reside. In this case, API Gateway can send requests to OSS over the internal network.

> **Note**
>
> To allow API Gateway to access OSS, you must grant permissions on your OSS bucket to API Gateway as prompted after you configure backend service information.

In the preceding figure, you can grant the read permissions on the entire bucket or a specific object to API Gateway because you set the Action parameter to GetObject. The read, write, and delete permissions that you can grant vary based on the value of the Action parameter. To remove the granted permissions, perform the following steps: Log on to the OSS console and click your OSS bucket in the left-side navigation pane. In the left-side navigation pane of the bucket details page, click Access Control. On the Access Control page, click Configure in the Bucket Policy section. On the Bucket Policy page, you can remove the granted permissions.

Step 8: Configure response information for the API

In this step, configure response information to generate API documentation. The documentation helps API callers better understand APIs. You can set parameters such as Response ContentType, Response Example, and Error Response Example. In this example, this step is skipped. Click Create.

Step 9: Publish the API

After you click Create, a message appears to inform you that the API is created, as shown in the following figure. API Gateway provides three environments to which you can publish an API: Release, Staging, and Test. All configurations you perform on an API can take effect only after you publish the API to a required environment. In this example, click Publish in the message that indicates successful API creation. In the Publish API dialog box, set the Stage parameter to Release, enter remarks, and then click Publish.

5. Create an APP and grant the APP the permissions to call the API

APPs are the identities that you use to call APIs. In Step 5, the Security Authentication parameter is set to Alibaba Cloud APP. Therefore, after you publish the API, you must create an APP and grant the APP the permissions to call the API.

Step 10: Create an APP

In the left-side navigation pane, choose `Call APIs` > `Apps`. On the Apps page, click Create App. In the Create App dialog box, enter an APP name and click Confirm. In the APP list, click the name of the created APP. Two authentication modes are provided: an AppKey and AppSecret pair and AppCode. In this example, the AppCode mode is used to authenticate the APP. For more information about this mode, see Call an API operation by using an AppCode.

Step 11: Grant the APP the permissions to call the API

In the left-side navigation pane, choose Open API > APIs. On the APIs page, find the created API and choose More > Authorize. A dialog box appears, as shown in the following figure. Set the Stage parameter to the environment to which you have published the API. In this example, set this parameter to Release. Enter the name of the APP you created in the search bar of the Choose Apps for Authorization section. In the search result, select the created APP, click Add in the Actions column, and then click Confirm. A message appears to inform you that the APP is authorized to call the API.

6. Debug the API

API Gateway supports online debugging. We recommend that you use this feature to check whether an API is correctly configured before you call this API on clients.

Step 12 Debug the API

On the `APIs` page, click the name of the created API. On the API details page, click `Debug API` in the left-side navigation pane. The following figure shows the page that appears. If you have defined request parameters for the API, you can enter different values for the request parameters to check whether the API is correctly configured.

When you debug the API, make sure that the App Name parameter is set to the authorized APP. The environment for debugging must be the one where the APP is authorized to call the API. Otherwise, the debugging may fail. In this example, select Release as the environment for debugging.

7. Call the API

After you perform the preceding steps, you have created the API and the APP, authorized the APP to call the API, debugged the API, and published the API to the online environment. In this step, you can call the API in your business system by using the AppCode.

Step 13: Call the API

For more information about API calls, see Overview. In this example, the curl command is used to call the API.

The following figure shows the call result.

3.Create an API operation with a resource in a VPC as the backend service

This topic describes how to create and publish an API operation with a resource in a VPC as the backend service in API Gateway, and how to call the API operation in an application by using an AppCode. The AppCode is automatically generated for the application when you set the authentication method of the API operation to Alibaba Cloud APP.

Overview

You must perform the following steps in sequence:

- Authorize API Gateway to access a VPC
- Create an API group
- Create and define an API operation
- Create an application and authorize the API operation
- Allow outbound IP addresses of API Gateway in a security group
- Debug the API operation
- Call the API operation

1. Create instances in a VPC.

Purchase and create SLB and ECS instances in a VPC.

In this example, an ECS instance in a VPC is used as the backend service of an API operation. The ECS instance is deployed in NGINX and uses port 80 for communication. Web services are deployed on the ECS instance.

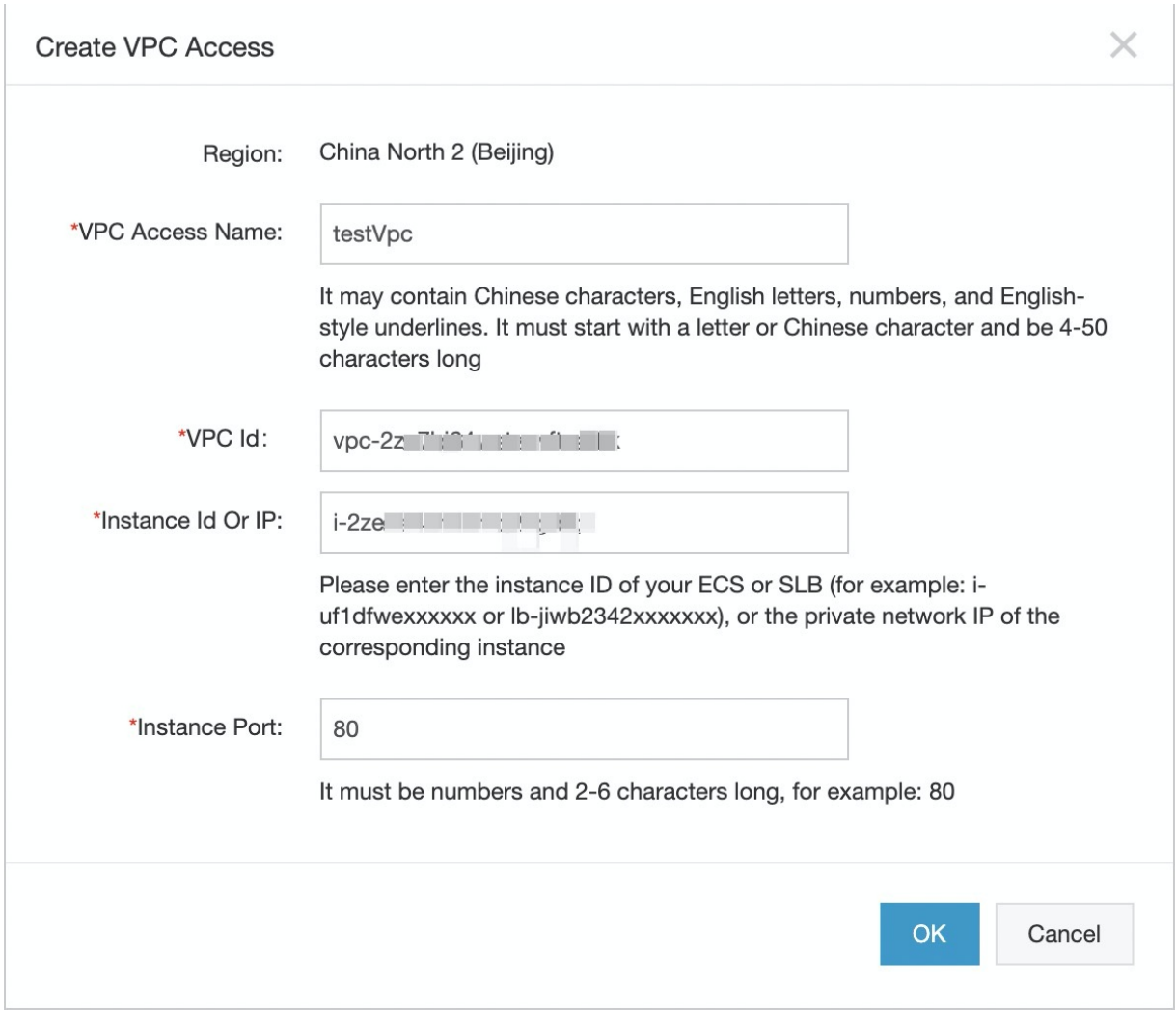
2. Authorize API Gateway to access the VPC

Create VPC access authorization.

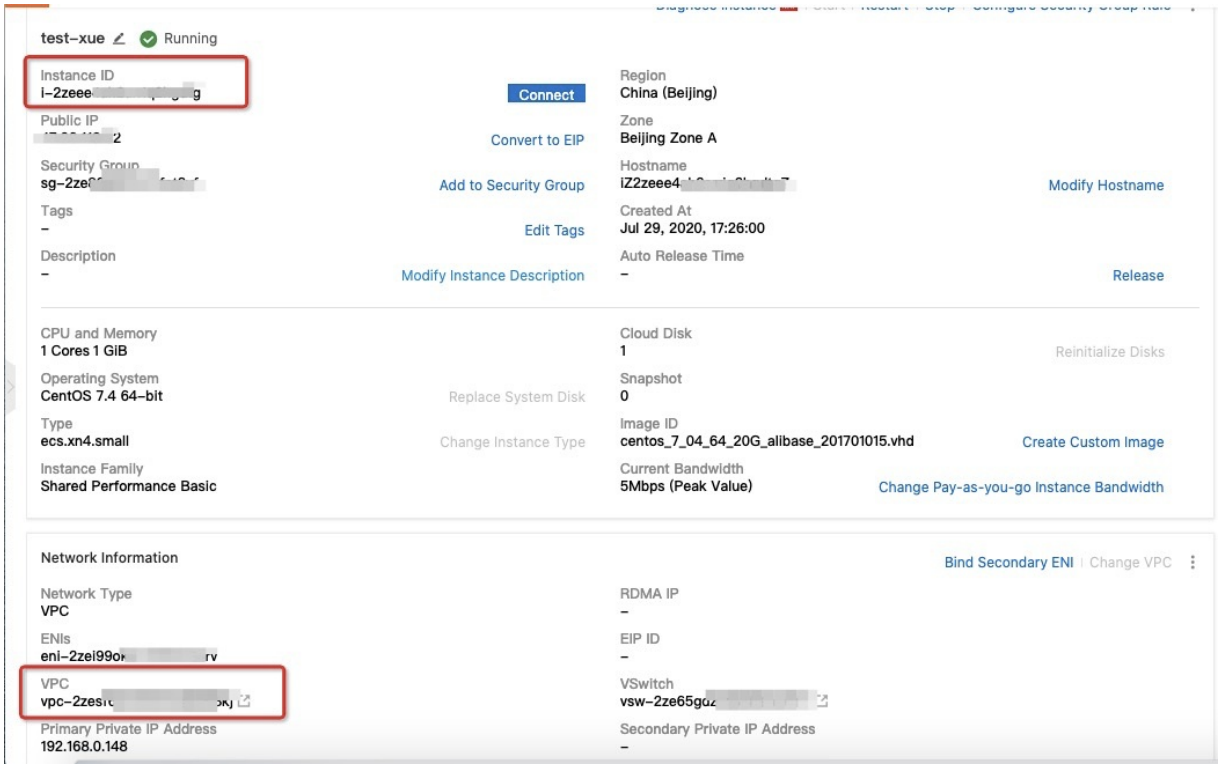
To allow API Gateway to access a VPC, you must create VPC access authorization.

In the left-side navigation pane of the API Gateway console, choose `Publish APIs` > `VPC Access`.

On the VPC Access List page, select the region where the VPC resides and click `Create VPC Access`. In the Create VPC Access dialog box, enter testVpc in the VPC Access Name field and specify VPC Id, Instance Id Or IP, and Instance Port.



VPC Id is the ID of the VPC where your backend service resides. Instance Id Or IP is the ID or private IP address of the instance where your backend service resides. You can obtain the information in the instance details.



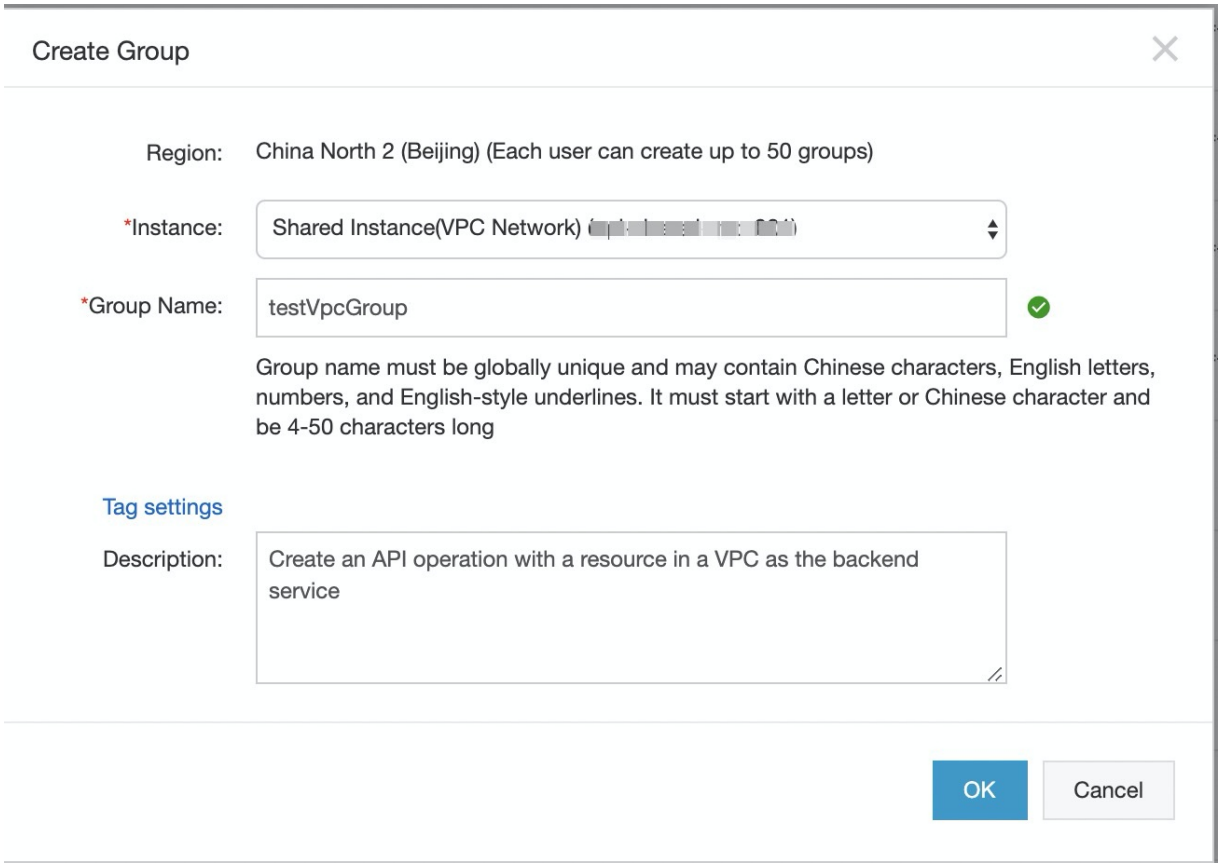
3. Create an API group

API Gateway allows you to manage API operations based on API groups. Before you create an API operation, you must create an API group.

Step 1: Create an API group.

Log on to the API Gateway console. In the left-side navigation pane, choose `Publish APIs` > `API Groups`. Select a region in the top navigation bar and click Create Group on the Group List page.

In the Create Group dialog box, select the instance to which the API group to be created belongs and enter the group name. In this example, set the Instance parameter to Shared Instance(VPC Network) (api-shared-vpc-001) and enter testVpcGroup in the Group Name field.



Step 2: View details of the API group.

After you create the API group, the API group appears on the Group List page. You can click the group name to go to the Group Details page. On this page, you can bind a domain name, modify basic information, and change the instance type.

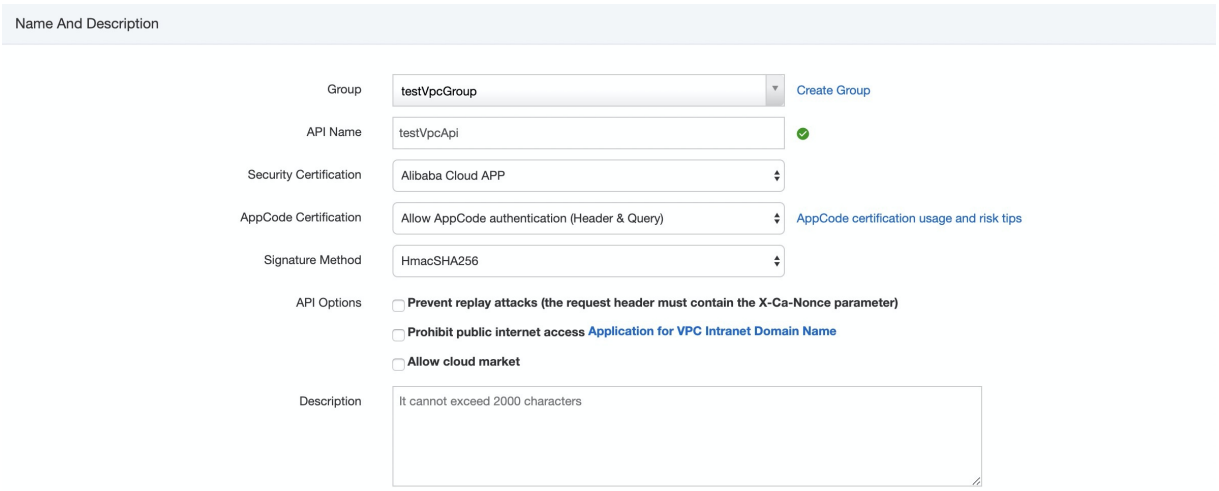
After an API group is created, API Gateway automatically creates a **public second-level domain name** for the API group. This default second-level domain name can be used only to test API calls and can be used for a maximum of **1,000 times** per day. We recommend that you bind **an independent domain name** after you create an API group. In this example, the default second-level domain name is used.

4. Create an API operation

In the left-side navigation pane, choose `Publish APIs` > `APIs`. Make sure that the current region is the region where the API group you created resides. On the API List page, click Create API.

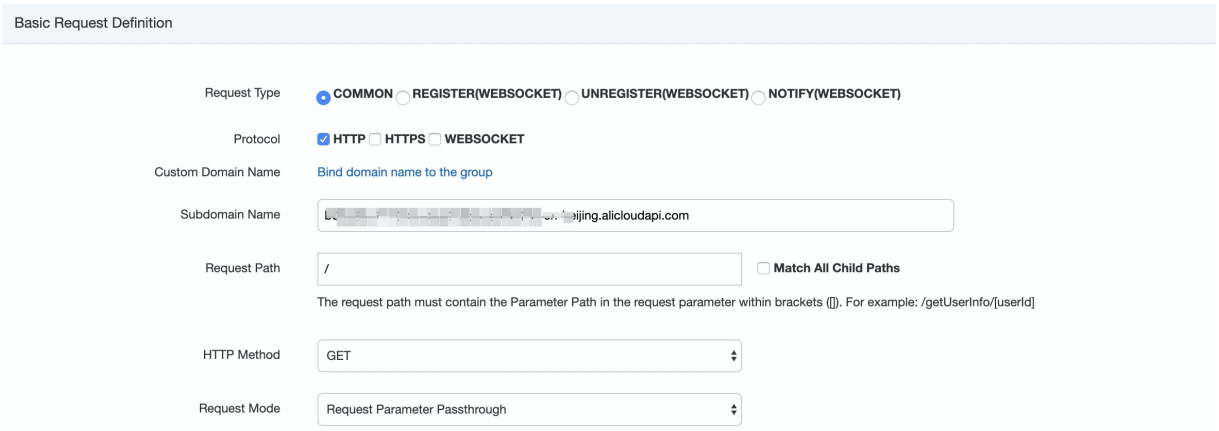
Step 1: Configure basic information for the API operation.

In this step, configure the basic information for the API operation to be created, including the API group to which the API operation belongs and the name, authentication method, type, and description of the API operation. In this example, set the Group parameter to the API group you created and the AppCode Certification parameter to **Allow AppCode authentication (Header & Query)**. Set other parameters as required and click Next.



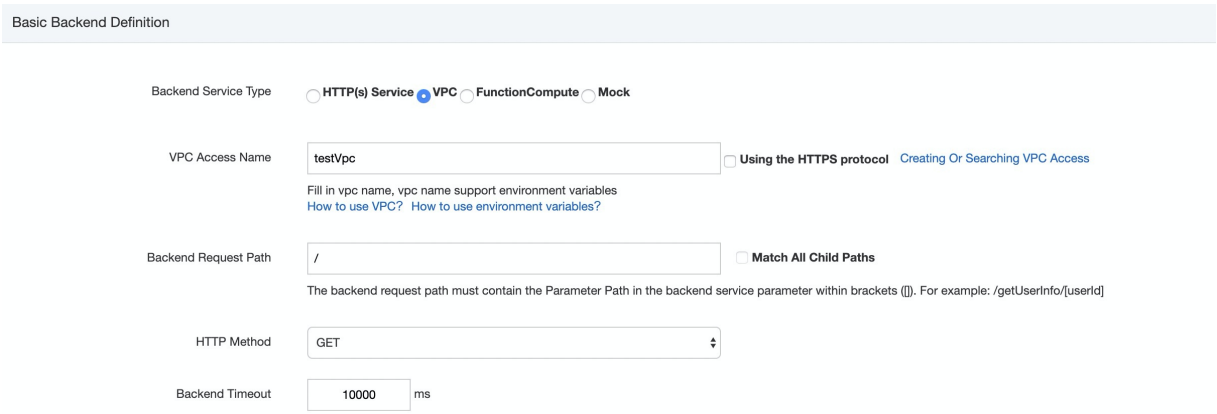
Step 2: Configure request information for the API operation.

In this step, define how a client, such as a browser, a mobile app, or a business system, sends a request for the API operation. The parameters to be configured in this step include Request Type, Protocol, Request Path, HTTP Method, Request Mode, and those in the Input Parameter Definition section. In this example, set the Request Mode parameter to **Request Parameter Passthrough**, which indicates that API Gateway passes API requests to the backend service in the VPC without processing them.



Step 3: Configure backend service information for the API operation.

In this step, configure a backend service type and address for the API operation and the mapping between request and response parameters. In this example, specify **VPC** for Backend Service Type, enter the VPC access name you created in the "Authorize API Gateway to access the VPC" section in the VPC Access Name field, specify Backend Request Path, and then click Next.

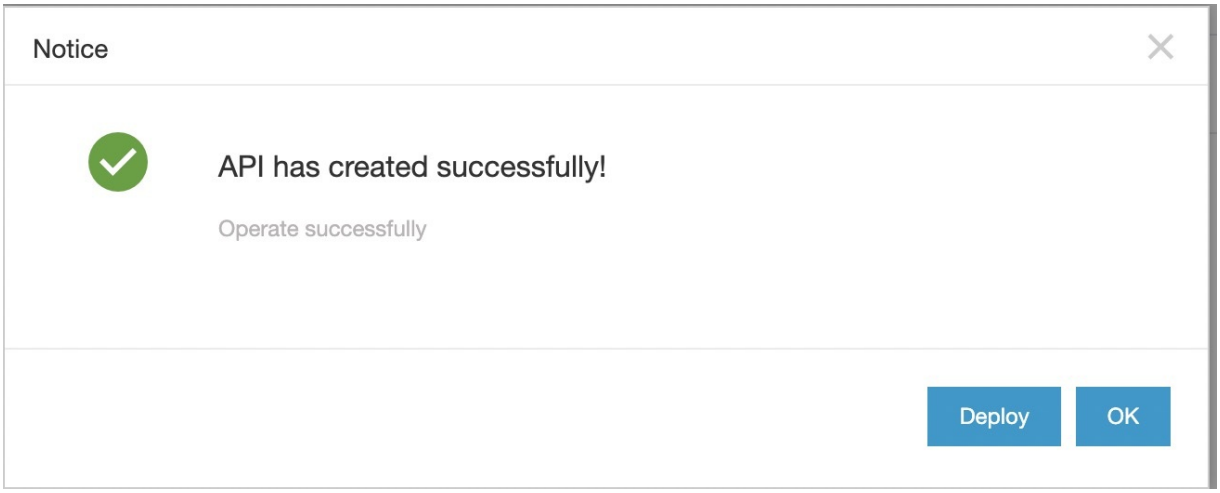


Step 4: Configure response information for the API operation.

In this step, configure response information to generate an API reference in the Alibaba Cloud API Gateway documentation. This API reference can help API users better understand the API operation. You can configure parameters such as ContentType of Response, Sample of Returned Results, and Sample of Returned Failure. Parameter configuration is not required in this example. Click `Create`.

Step 5: Publish the API operation.

After the preceding operation is successful, a message appears to inform you that the API operation is modified. All configurations of the API operation take effect only after you publish the API operation. API Gateway provides three environments to which you can publish an API operation: Release, Pre, and Test. In this example, click `Deploy` in the message. In the dialog box that appears, set the Select The Stage To Release To parameter to Release, enter your remarks, and then click Deploy.

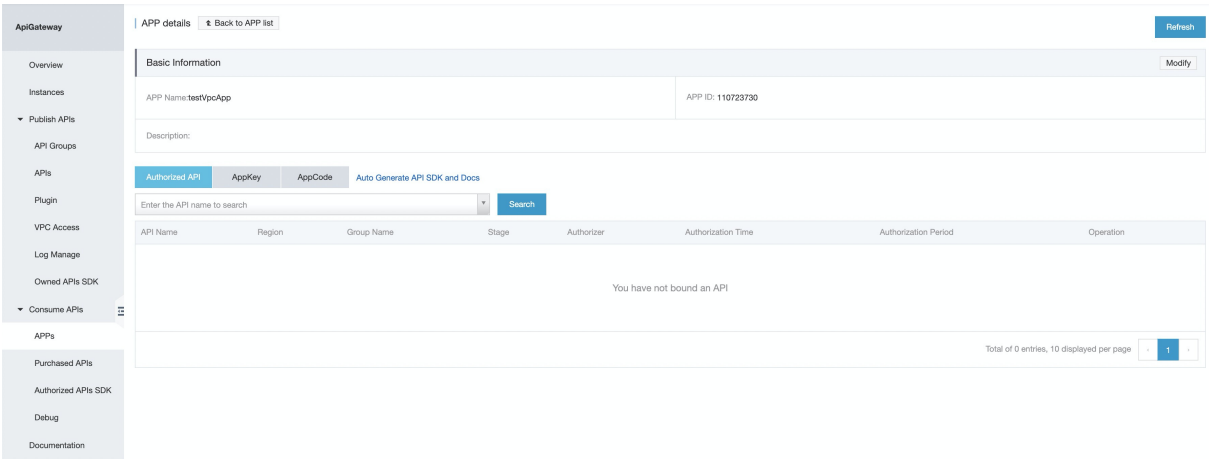


5. Create and authorize an application

Applications are identities that you use to call API operations. In Step 1 of the "Create an API operation" section, the Security Certification parameter is set to Call an API operation by using an AppCode. Therefore, after you publish the API operation, you must create and authorize an application for calling the API operation.

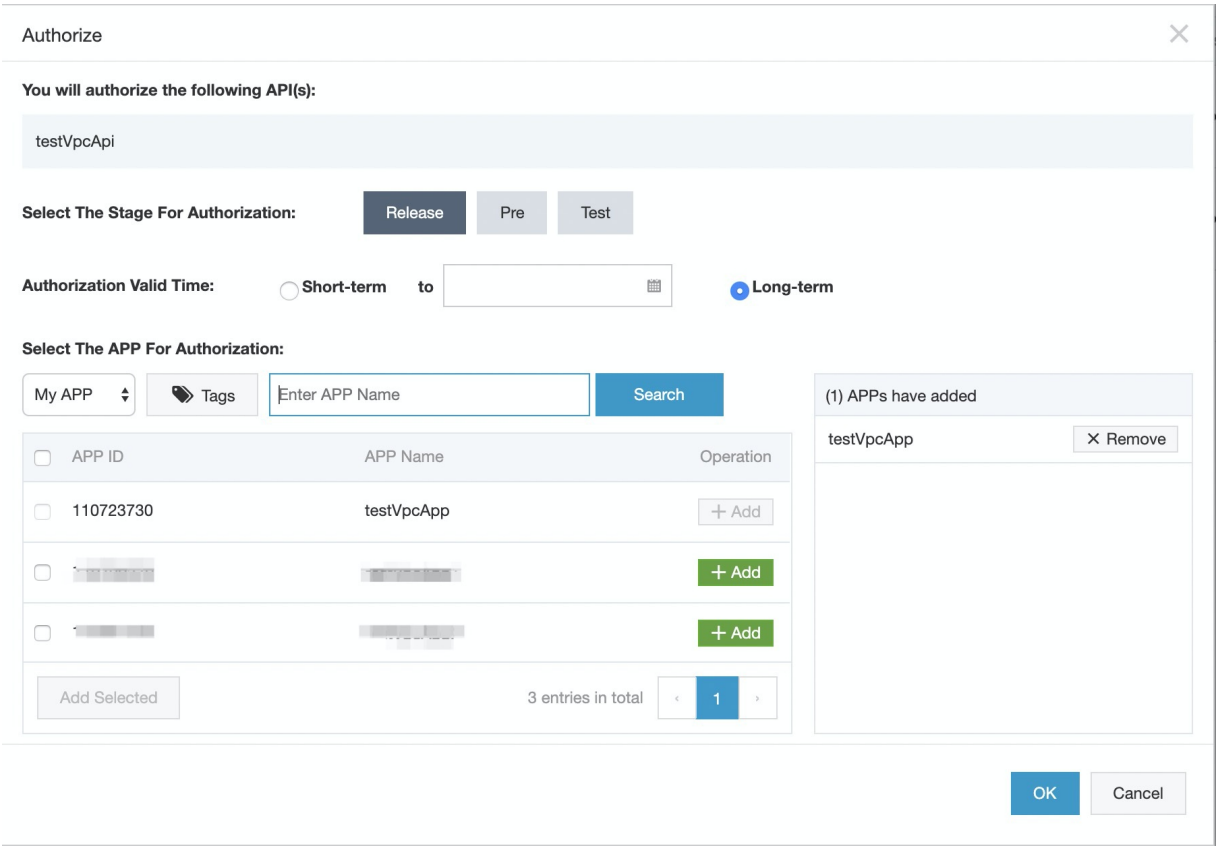
Step 1: Create an application.

In the left-side navigation pane, choose `Consume APIs` > `APPs`. On the APP List page, click Create APP. In the Create APP dialog box, enter an application name and click OK. In the application list, click the name of the application you created. Two authentication modes are provided for the applications of an API operation whose Security Certification parameter is set to Alibaba Cloud APP: AppKey and AppCode, as shown in the following figure. In this example, the AppCode mode is used to authenticate the application. For more information about the security certification method Alibaba Cloud APP, see Call an API operation by using an AppCode.



Step 2: Authorize the API operation.

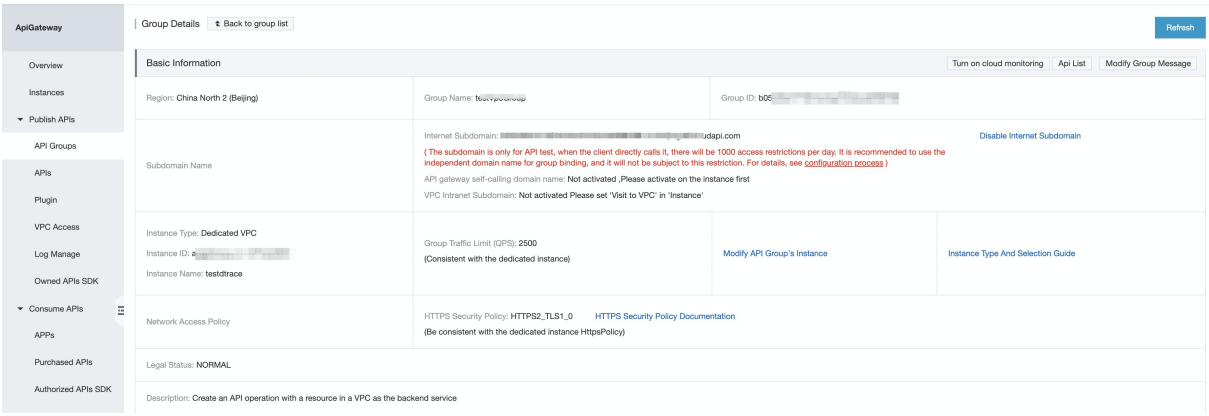
In the left-side navigation pane, choose Publish APIs > `APIs`. On the API List page, find the API operation you created and click `Authorize` in the Operation column. A dialog box appears, as shown in the following figure. Set the Select The Stage For Authorization parameter to the environment to which you have published the API operation. In this example, set this parameter to Release. Enter the name of the application you created in the search bar of the Select The APP For Authorization section. In the search result, select the application you created, click Add in the Operation column, and then click OK. A message appears to inform you that the application is authorized to call the API operation.



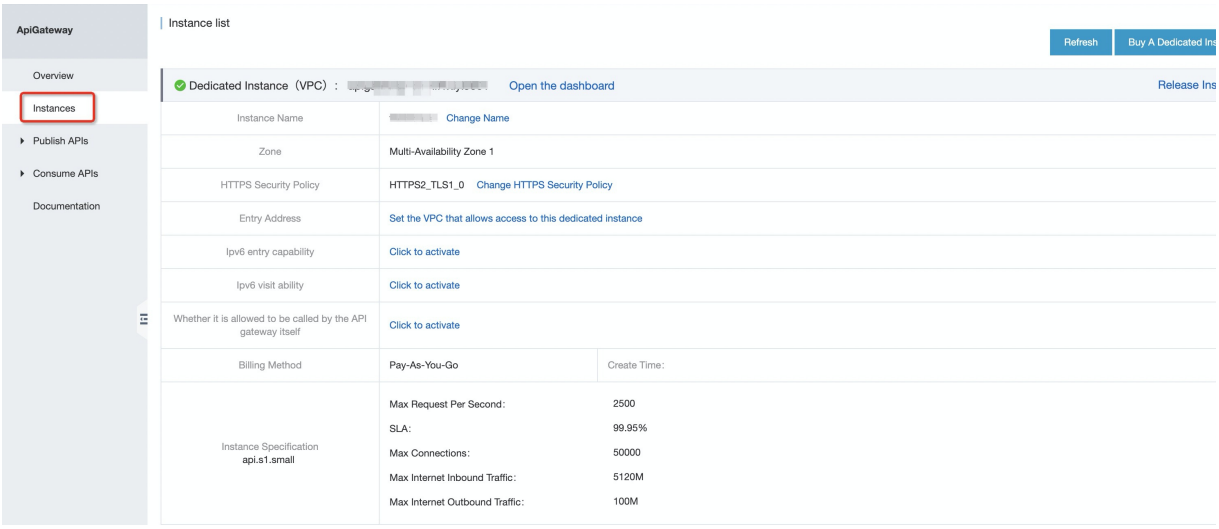
6. Allow outbound IP addresses of API Gateway in a security group

If the security group of your ECS instance does not allow all CIDR blocks over a specified port, you must add the outbound IP addresses of API Gateway to the security group to allow these IP addresses.

The outbound IP address of an API group is the outbound IP address of the instance to which the API group belongs. To obtain the outbound IP address of an exclusive instance, log on to the API Gateway console. In the left-side navigation pane, choose Publish APIs > API Groups. On the Group List page, find the API group whose information you want to view and click the group name. On the Group Details page, view information about the instance to which the API group belongs.



In the left-side navigation pane, click Instances. On the Instance list page, view the information of the instance to which the API group belongs, as shown in the following figure. You can view the outbound IP address of a shared instance on the Instance list page.

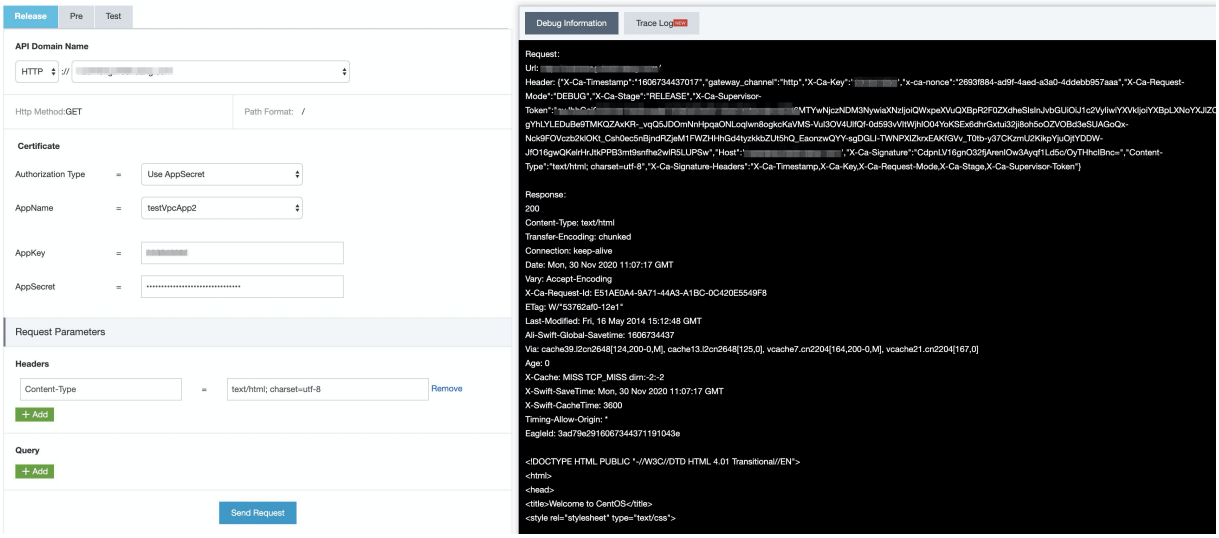


7. Debug the API operation

API Gateway supports online debugging. We recommend that you use this feature to check whether an API operation is correctly configured before you allow clients to call it.

On the `API List` page, find the API operation you created and click `Debug` in the Operation column. The following figure shows the page that appears. If you have defined request parameters for the API operation, you can enter different values for the request parameters to check whether the API operation is correctly configured.

When you debug the API operation, make sure that the AppName parameter is set to an authorized application. The Stage parameter must be set to the environment where the application is authorized. Otherwise, the debugging may fail. In this example, set the Stage parameter to RELEASE.



8. Call the API operation

In this example, curl is used to call the API operation. For more information, see Call an API operation by using an AppCode.

Note:The API operation in the release environment is called by default.

For information about the environments of API operations, see Configure different environments for an API operation.

The main purpose of this topic is to help you quickly get started. The high availability of a backend service is not considered. If you have any questions, see Use a resource in a VPC as the backend service of an API operation.

4.Create an API operation with HTTP as the backend service

This topic describes how to create and publish an API operation with HTTP as the backend service in API Gateway, and how to call the API operation in an application by using an AppKey and an AppSecret. The AppKey and AppSecret are automatically generated for the application provided that you set the authentication method of the API operation to Alibaba Cloud APP.

1. Overview

You must perform the following steps in sequence:

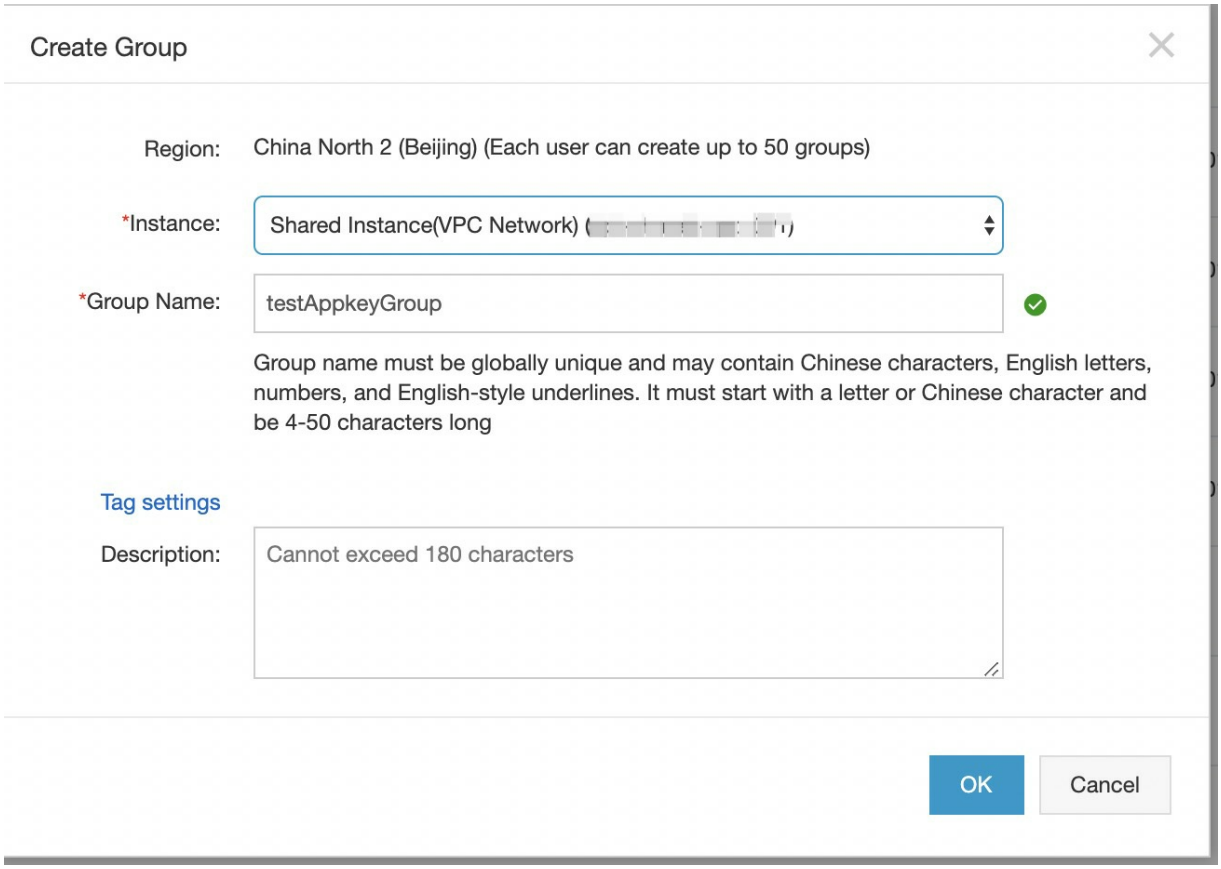
- Create an API group
- Create an API operation
- Create and authorize an application
- Debug the API operation
- Call the API operation

2. Create an API group

In API Gateway, API operations are managed in API groups. Before you create an API operation, you must create an API group.

Step 1: Create an API group

Log on to the API Gateway console. In the left-side navigation pane, choose `Publish APIs` > `API Groups`. Select a region in the top navigation bar and click Create Group on the Group List page. In the Create Group dialog box, select an instance to which the API group to be created belongs and enter a group name. In this example, set the Instance parameter to Shared Instance(VPC Network)(api-shared-vpc-001) and enter testAppkeyGroup in the Group Name field.



Step 2: View details of the API group

After you create the API group, the API group appears on the Group List page. You can click the group name to go to the details page, where you can perform operations such as binding a domain name, modifying basic information, and changing the instance type.

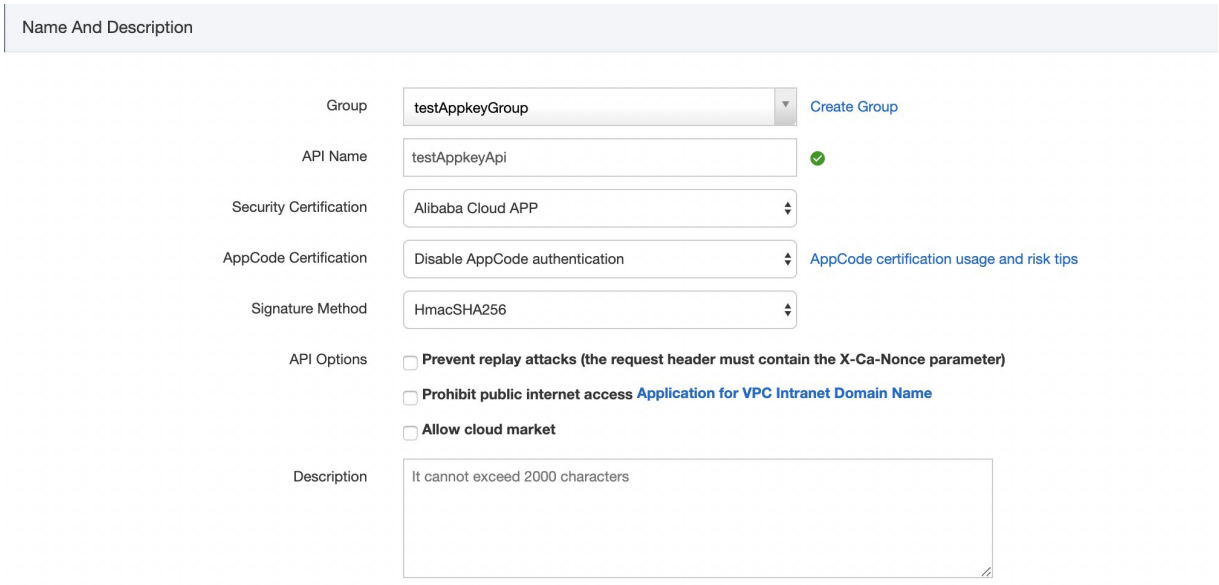
After an API group is created, API Gateway automatically creates a public second-level domain name for the API group. This default second-level domain name can only be used for testing API calls and can be used for a maximum of 1,000 times per day. We recommend that you bind an independent domain name after you create an API group. In this example, the default second-level domain name for testing API calls is used.

3. Create an API operation

In the left-side navigation pane, choose `Publish APIs` > `APIs`. Make sure that the current region is the same region where the API group you created resides. On the API List page, click Create API.

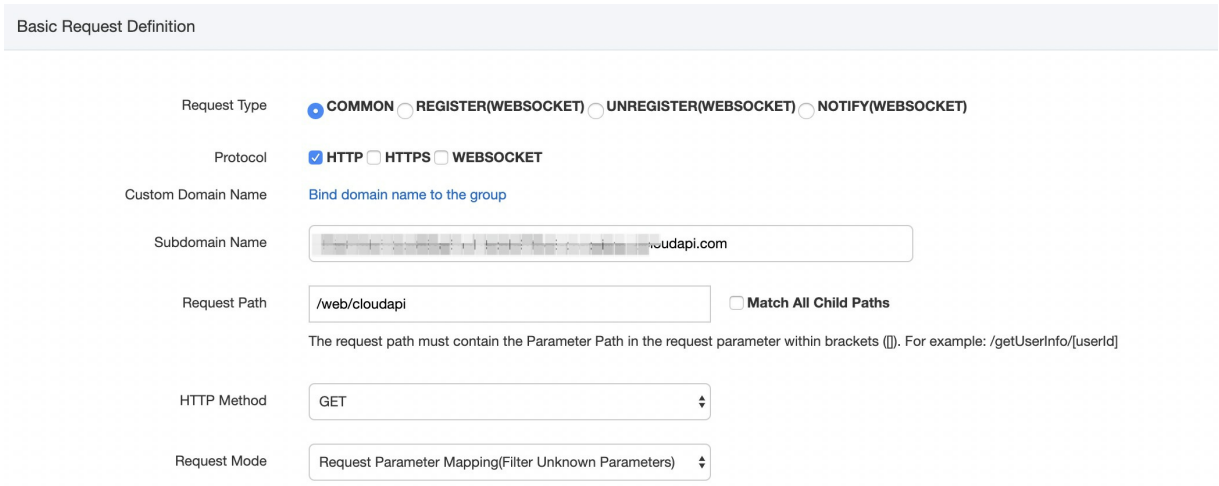
Step 3: Configure basic information for the API operation

In this step, configure the basic information for the API operation to be created, including the API group to which the API operation belongs and the name, authentication method, and description of the API operation. In this example, set the Group parameter to testAppkeyGroup, the Security Certification parameter to Alibaba Cloud APP, and the AppCode Certification parameter to Disable AppCode authentication. Set other parameters as required and click Next.



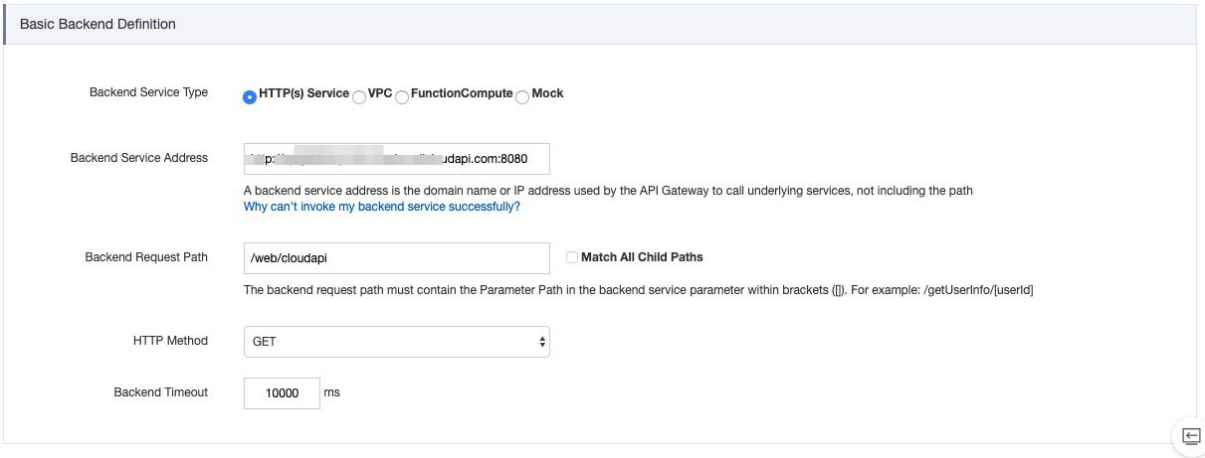
Step 4: Configure request information for the API operation

In this step, define how a client, such as a browser, a mobile app, or a business system, sends a request for the API operation. The parameters to be set in this step include Request Type, Protocol, Request Path, HTTP Method, Request Mode, and those in the Input Parameter Definition section. In this example, enter /web/cloudapi in the Request Path field and do not define request parameters.



Step 5: Configure backend service information for the API operation

In this step, configure a backend service type and address for the API operation and the mapping relationship between request and response parameters. In this example, set the Backend Service Type parameter to HTTP(s) Service. The backend service address must be accessible on Alibaba Cloud networks and the Internet. For information about other backend service types, see API Gateway documentation. Set other parameters such as Backend Service Address and Backend Request Path as prompted.

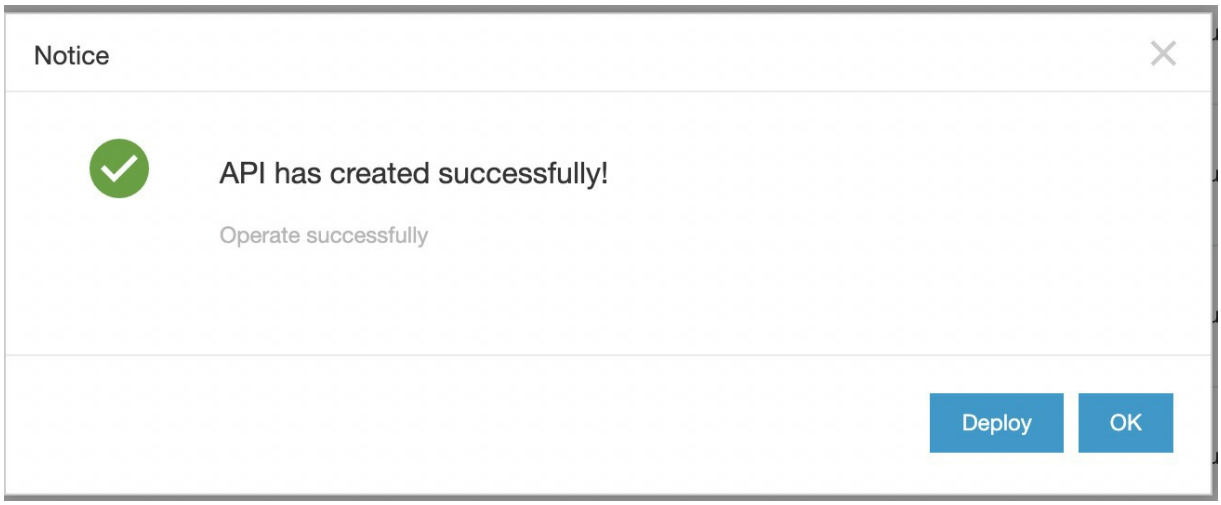


Step 6: Configure response information for the API operation

In this step, configure response information to generate an API reference in Alibaba Cloud API Gateway SDK. This API reference can help API users better understand the API operation. You can set parameters such as ContentType of Response, Sample of Returned Results, and Sample of Returned Failure. In this example, this step is skipped. Click `Create`.

Step 7: Publish the API operation

After you create or modify the API operation, a message appears to inform you that the API operation is created or modified. All configurations of the API operation take effect only after you publish the API operation. API Gateway provides three environments to which you can publish an API operation: Release, Pre, and Test. In this example, click `Deploy` in the message. In the dialog box that appears, set the Select The Stage To Release To parameter to Release, enter your remarks, and then click Deploy.

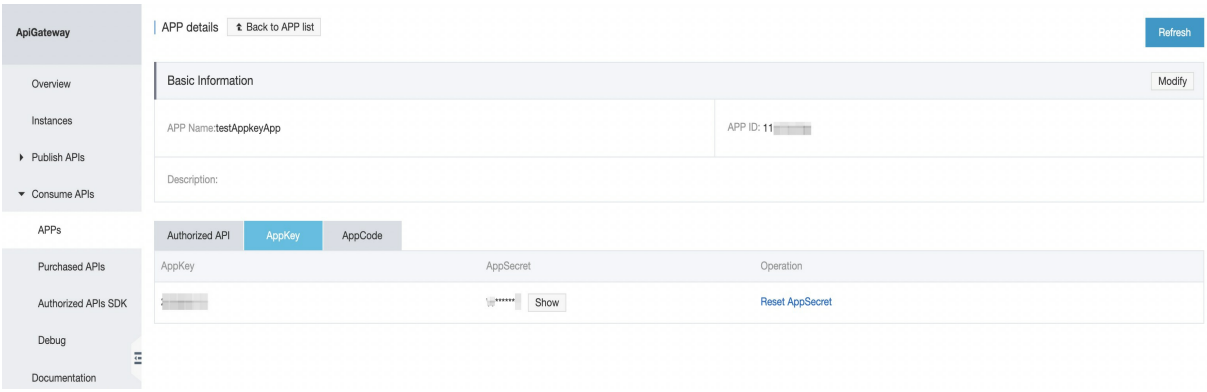


4. Create and authorize an application

Applications are identities that you use to call API operations. In step 3, the Security Certification parameter is set to Alibaba Cloud APP. Therefore, after you publish the API operation, you must create and authorize an application for calling the API operation.

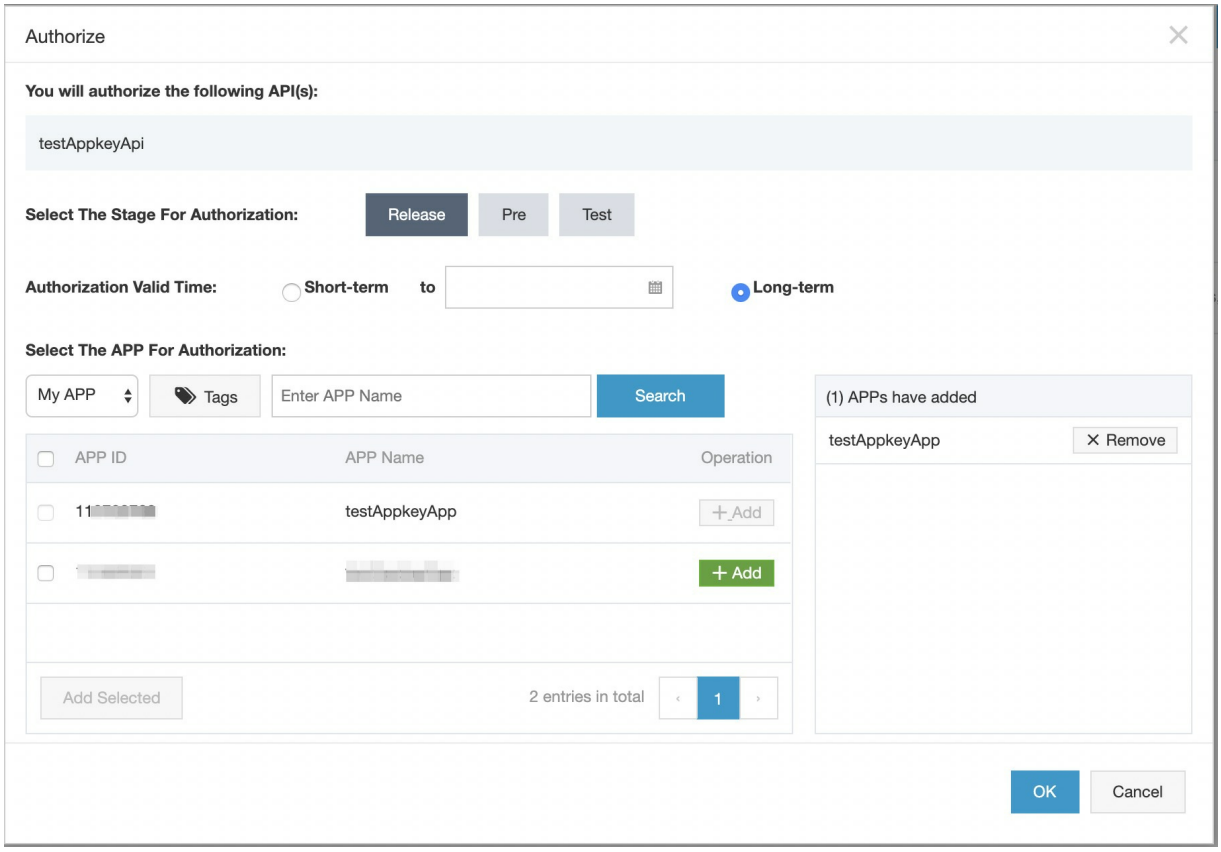
Step 8: Create an application

In the left-side navigation pane, choose `Consume APIs` > `APPs`. On the APP List page, click Create APP. As shown in the following figure, for an API operation whose Security Certification parameter is set to Alibaba Cloud APP, two authentication modes are provided for its applications: AppKey and AppCode. The AppKey mode provides a key pair that consists of an AppKey and an AppSecret. You can regard them as an account and a password. When you call the API operation, you must specify the AppKey as a request parameter. The AppSecret is used to calculate the signature string. API Gateway authenticates the key pair to verify your identity. For more information about the Alibaba Cloud APP authentication method, see Call an API operation by using an AppCode.



Step 9: Authorize the application

In the left-side navigation pane, choose Publish APIs > `APIs`. On the API List page, find the API operation you created and click `Authorize` in the Operation column. A dialog box appears, as shown in the following figure. Set the Select The Stage For Authorization parameter to the environment to which you have published the API operation. In this example, set this parameter to Release. Search for the application you created, click Add, and then click OK. A message appears to inform you that the application is authorized to call the API operation.



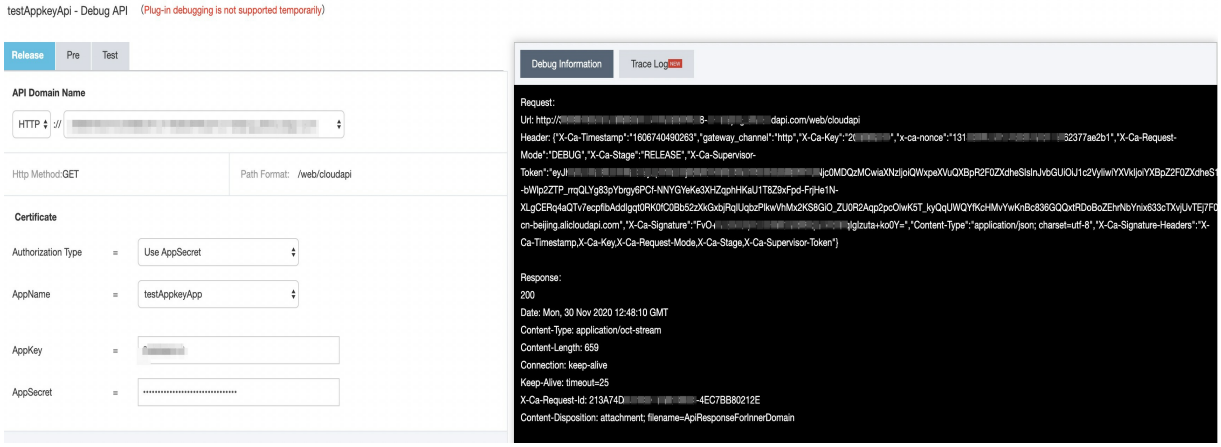
5. Debug the API operation

API Gateway supports online debugging. We recommend that you use this feature to check whether an API operation is correctly configured before you allow it to be called on clients.

Step 10: Debug the API operation

On the `API List` page, find the API operation you created and click `Debug` in the Operation column. A page appears, as shown in the following figure. If you have defined request parameters for the API operation, you can enter different values for the request parameters to check whether the API operation is correctly configured.

When you debug the API operation, make sure that the AppName parameter is set to an authorized application. The Stage parameter must be set to the environment where the application is authorized, otherwise the debugging may fail. In this example, set the Stage parameter to RELEASE.

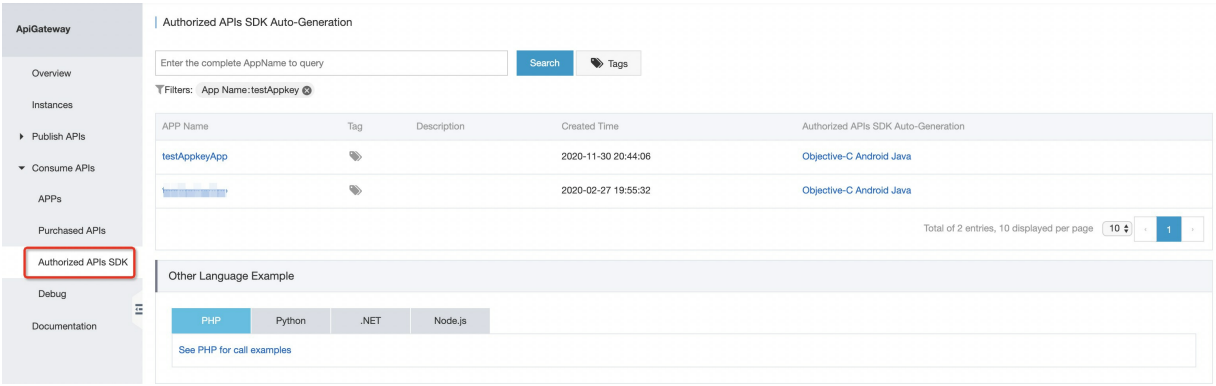


6. Call the API operation

Now you have created the API operation and the application, authorized the application to call the API operation, debugged the API operation, and published the API operation to the online environment. In this step, you can download Alibaba Cloud API Gateway SDK for the API operation and use the SDK to call the API operation in your business system.

Step 11: Call the API operation

In the left-side navigation pane, choose `Consume APIs` > `Authorized APIs SDK`. On the Authorized APIs SDK Auto-Generation page, you can download the SDK that is used to call the API operation in the application. You can also download the SDK for other coding languages.



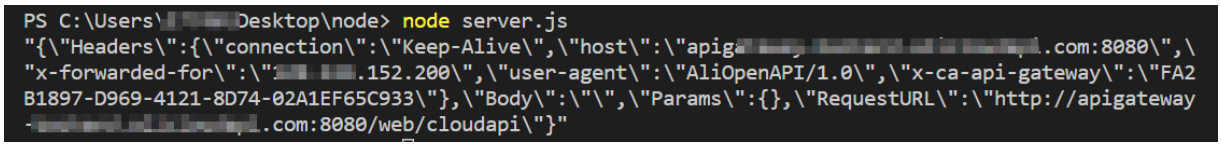
In this example, Alibaba Cloud API Gateway SDK for Node.js is used to call the API operation.

1. Use Node Package Manager (NPM) to install Alibaba Cloud API Gateway SDK for Node.js. Run the following command in NPM: `$ npm install aliyun-api-gateway -S`.

2. Replace YOUR_APP_KEY and YOUR_APP_SECRET in the following code snippet with the AppKey and AppSecret of the application that is created in this example.

```
// Import Alibaba Cloud API Gateway SDK for Node.js that you downloaded.
const Client = require('aliyun-api-gateway').Client;
// Create an instance of the authorized application. Specify the AppKey and AppSecret of th
e authorized application.
const client = new Client('YOUR_APP_KEY','YOUR_APP_SECRET');
async function get() {
// Use the domain name of the API group to which the API operation to be called belongs. Yo
u can use the public second-level domain name provided by API Gateway to test API calls, bu
t only for a limited number of times per day. We recommend that you bind an independent dom
ain name to the API Group.
  var url = 'YOUR_GROUP_DOMAIN';
  var result = await client.get(url, {
// Define the response format in the request header of the API operation. All responses of
the API operation will adhere to the defined response format. We recommend that you define
the response format based on your requirements.
    headers: {
      accept: 'application/json'
    },
  });
  console.log(JSON.stringify(result));
}
get().catch((err) => {
  console.log(err.stack);
});
```

The following figure shows a sample response.



5.Create an API operation with Function Compute as the backend service

This topic describes how to create and publish an API operation with Function Compute as the backend service in API Gateway, and how to call the API operation in an application by using an AppCode. The AppCode is automatically generated for the application provided that you set the authentication method of the API operation to Alibaba Cloud APP.

1. Overview

You must perform the following steps in sequence:

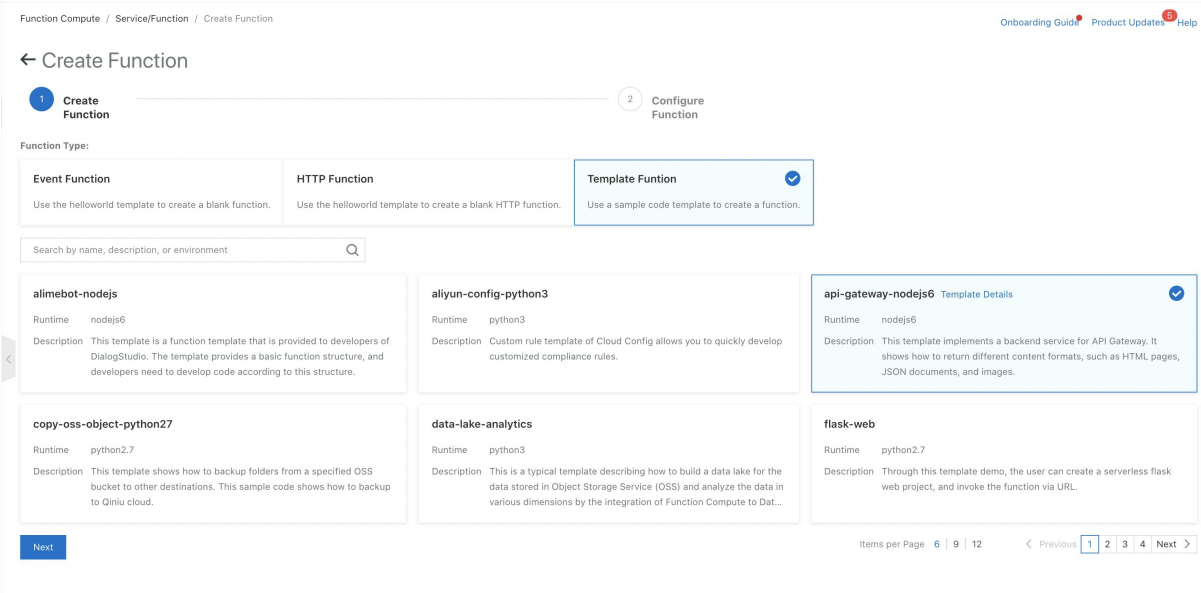
- Create a function in Function Compute
- Create an API group in API Gateway
- Create an API operation
- Create and authorize an application
- Debug the API operation
- Call the API operation

2. Create a function in Function Compute

Function Compute is an event-driven compute service. Functions are event-driven, that is, when an event occurs, the event triggers the execution of the corresponding function. API Gateway is an event source for Function Compute. After API Gateway receives a request for an API operation that uses Function Compute as the backend service, API Gateway triggers the execution of the corresponding function in Function Compute and Function Compute sends the execution results to API Gateway.

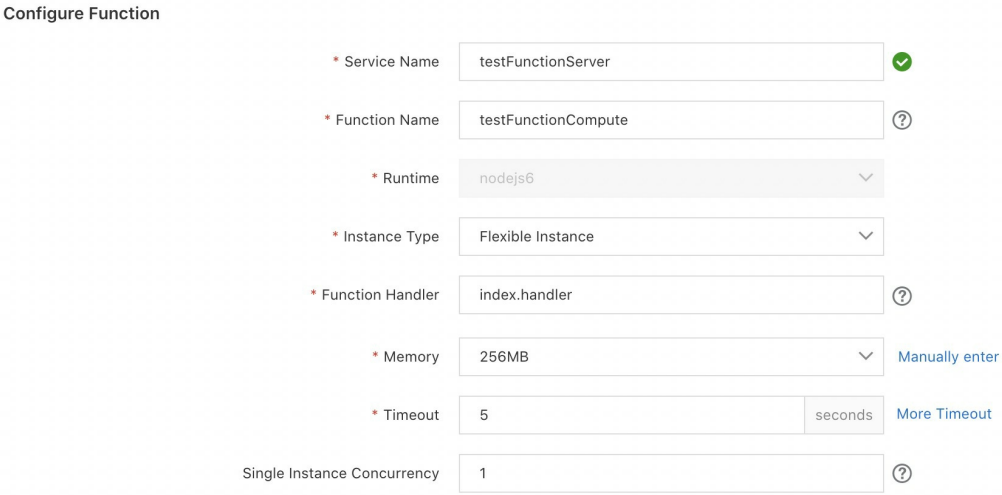
Step 1: Create a function by using the apigateway template in Function Compute

Log on to the Function Compute console. Select a region in the top navigation bar. In the left-side navigation pane, click `Service/Function`. On the page that appears, click `Create Function`. In the `Create Function` step, click `Template Function`. Then, select the `api-gateway-nodejs6` template and click Next. This template is used to create a function whose event source is API Gateway.



Step 2: Configure the function

For more information about how to configure a function, see Function Compute documentation. In this example, set the parameters as required, as shown in the following figure.

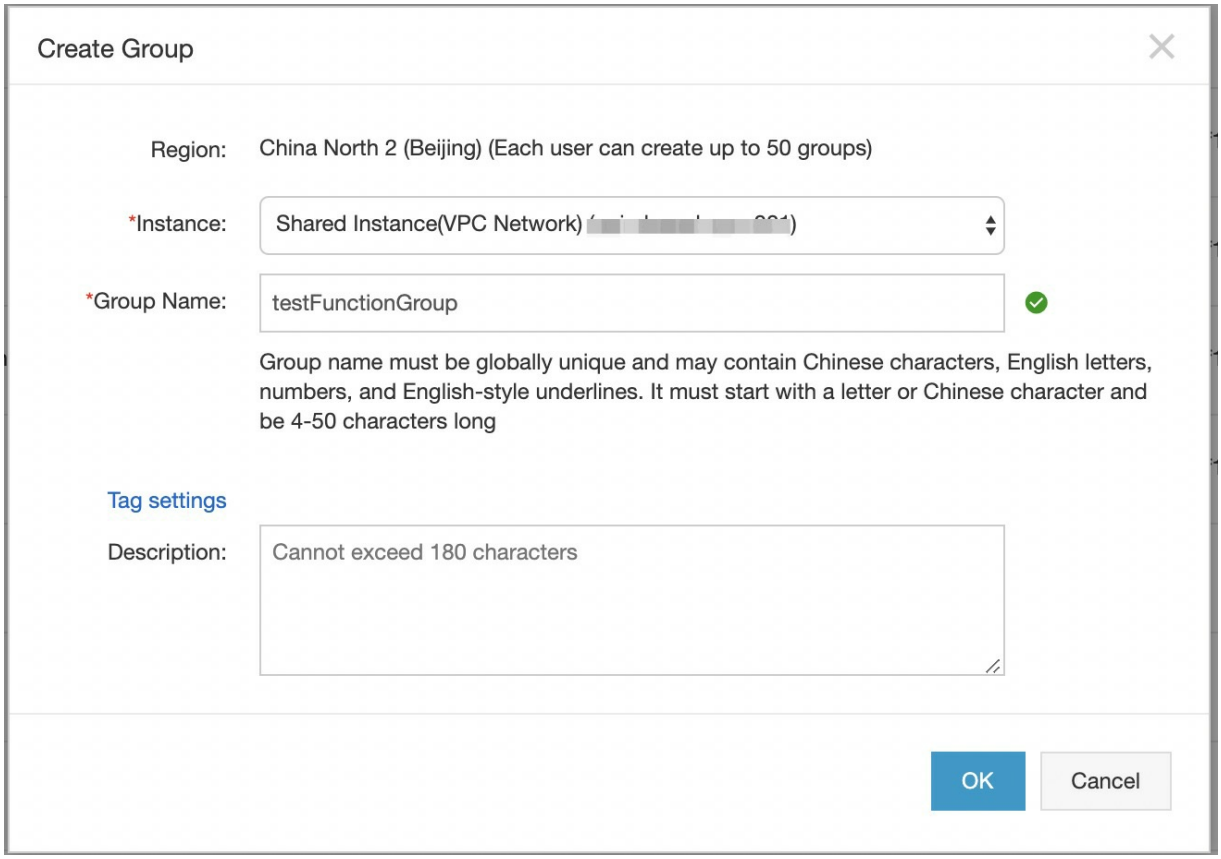


3. Create an API group in API Gateway

In API Gateway, API operations are managed in API groups. Before you create an API operation, you must create an API group.

Step 3: Create an API group in API Gateway

Log on to the API Gateway console. In the left-side navigation pane, choose `Publish APIs` > `API Groups`. Select a region in the top navigation bar and click Create Group on the Group List page. In the Create Group dialog box, select an instance to which the API group to be created belongs and enter a group name. In this example, set the Instance parameter to Shared Instance(VPC Network)(api-shared-vpc-001) and enter testFunctionGroup in the Group Name field. The API group must be in the same region as the function that you created in Function Compute.



Step 4: View details of the API group

After you create the API group, the API group appears on the Group List page. You can click the group name to go to the details page, where you can perform operations such as binding a domain name, modifying basic information, and changing the instance type.

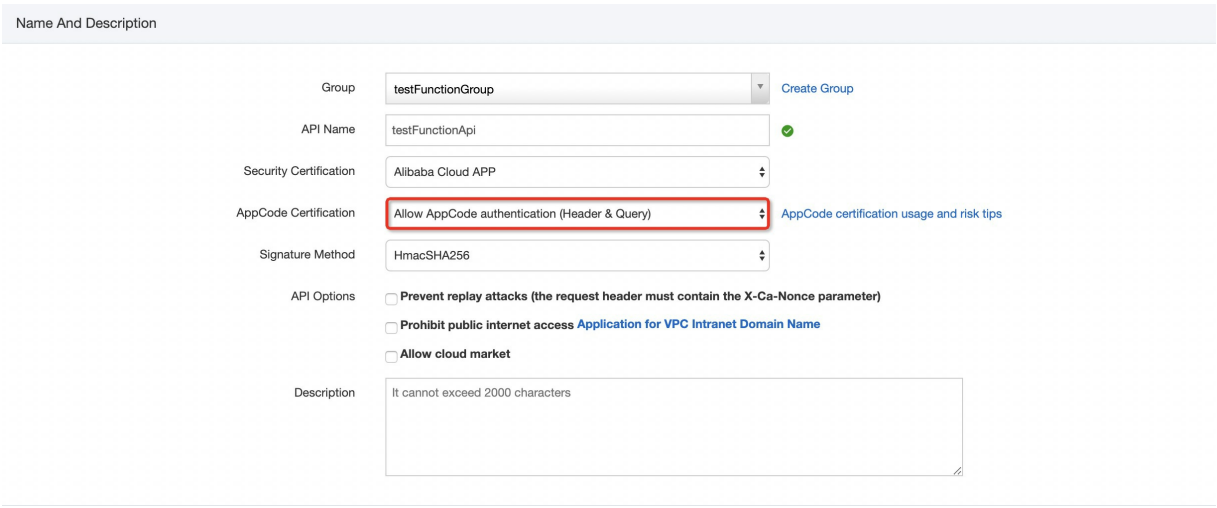
After an API group is created, API Gateway automatically creates a public second-level domain name for the API group. This default second-level domain name can only be used for testing API calls and can be used for a maximum of 1,000 times per day. We recommend that you bind an independent domain name after you create an API group. In this example, the default second-level domain name for testing API calls is used.

4. Create an API operation

In the left-side navigation pane, choose `Publish APIs` > `APIs`. Make sure that the current region is the same region where the API group you created resides. On the API List page, click Create API.

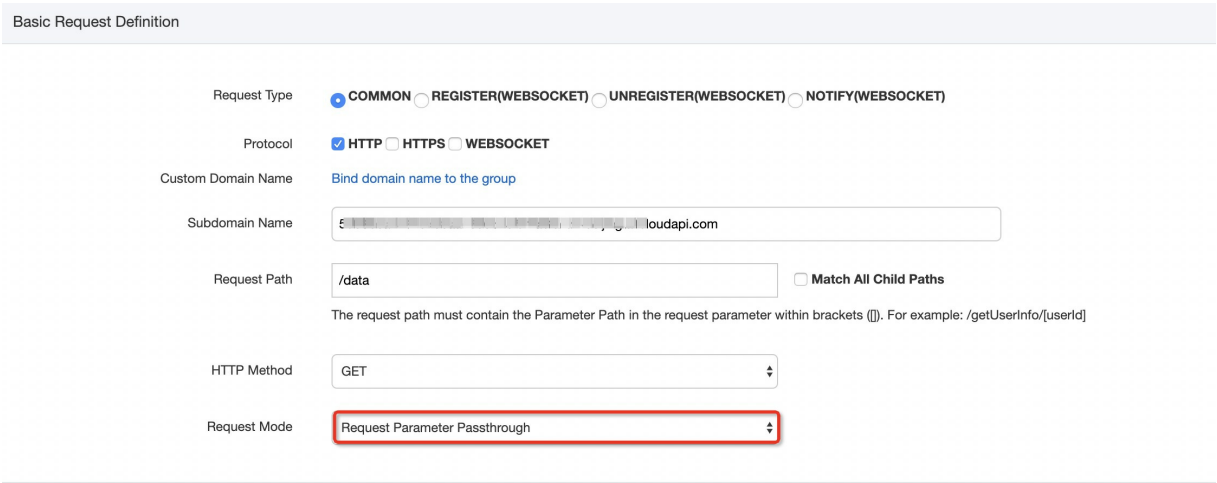
Step 5: Configure basic information for the API operation

In this step, configure the basic information for the API operation to be created, including the API group to which the API operation belongs and the name, authentication method, and description of the API operation. In this example, set the Group parameter to the API group you created and the AppCode Certification parameter to **Allow AppCode authentication (Header & Query)**. Set other parameters as required and click Next.



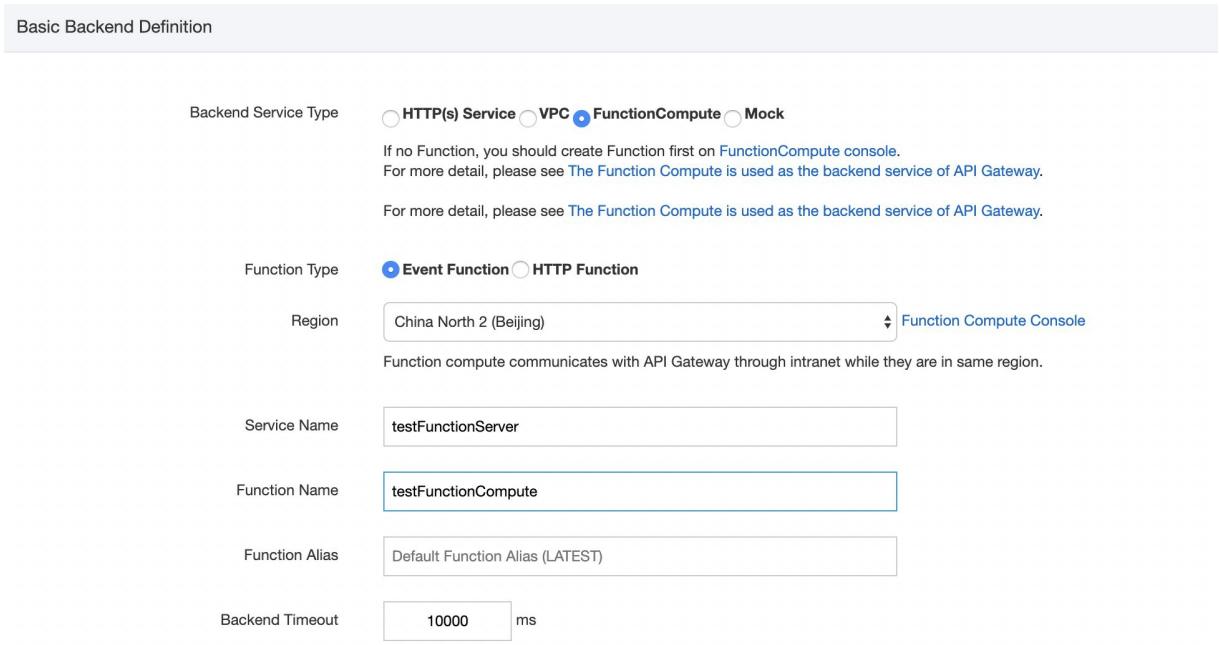
Step 6: Configure request information for the API operation

In this step, define how a client, such as a browser, a mobile app, or a business system, sends a request for the API operation. The parameters to be set in this step include Request Type, Protocol, Request Path, HTTP Method, Request Mode, and those in the Input Parameter Definition section. In this example, set the Request Mode parameter to **Request Parameter Passthrough**, which indicates that API Gateway does not process API requests and pass them directly to Function Compute.



Step 7: Configure backend service information for the API operation

In this step, configure a backend service type and address for the API operation and the mapping relationship between request and response parameters. In this example, set the Backend Service Type parameter to **FunctionCompute**. Configure other information, such as the name and service name of the function that you created in Function Compute, and click `Get Authorization`. Then, click Next.

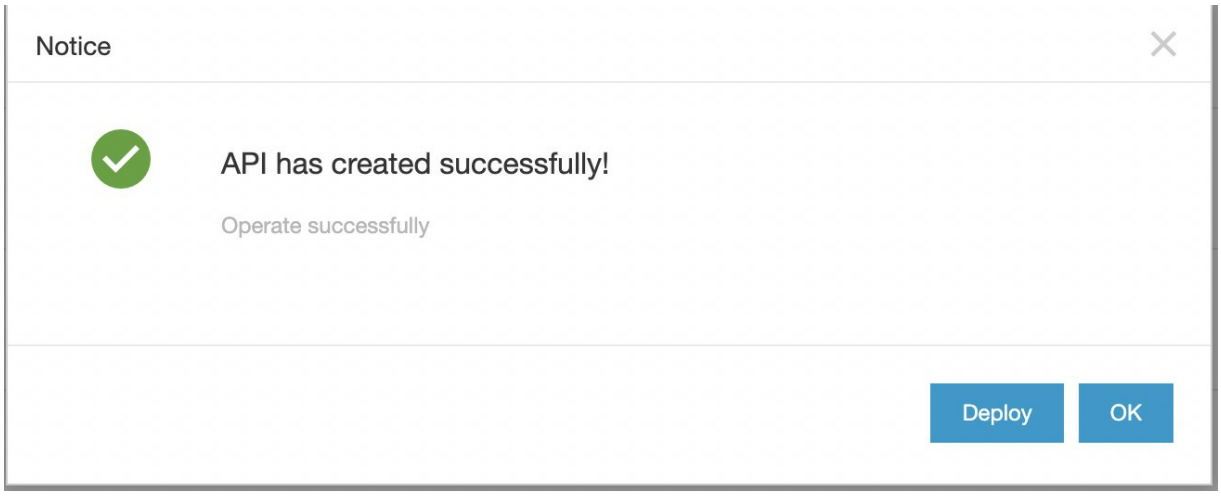


Step 8: Configure response information for the API operation

In this step, configure response information to generate an API reference in Alibaba Cloud API Gateway SDK. This API reference can help API users better understand the API operation. You can set parameters such as ContentType of Response, Sample of Returned Results, and Sample of Returned Failure. In this example, this step is skipped. Click `Create`.

Step 9: Publish the API operation

After you create or modify the API operation, a message appears to inform you that the API operation is created or modified. All configurations of the API operation take effect only after you publish the API operation. API Gateway provides three environments to which you can publish an API operation: Release, Pre, and Test. In this example, click `Deploy` in the message. In the dialog box that appears, set the Select The Stage To Release To parameter to Release, enter your remarks, and then click Deploy.

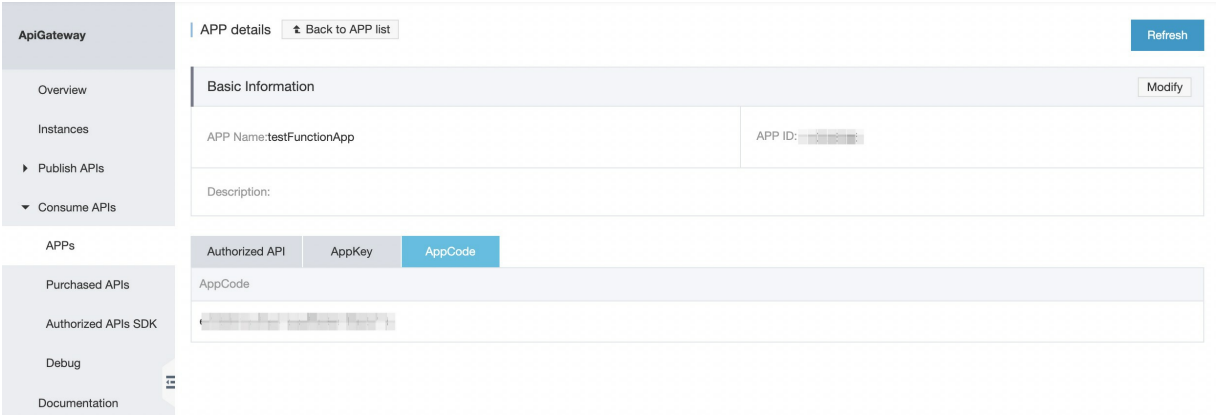


5. Create and authorize an application

Applications are identities that you use to call API operations. In step 5, the Security Certification parameter is set to Alibaba Cloud APP. Therefore, after you publish the API operation, you must create and authorize an application for calling the API operation.

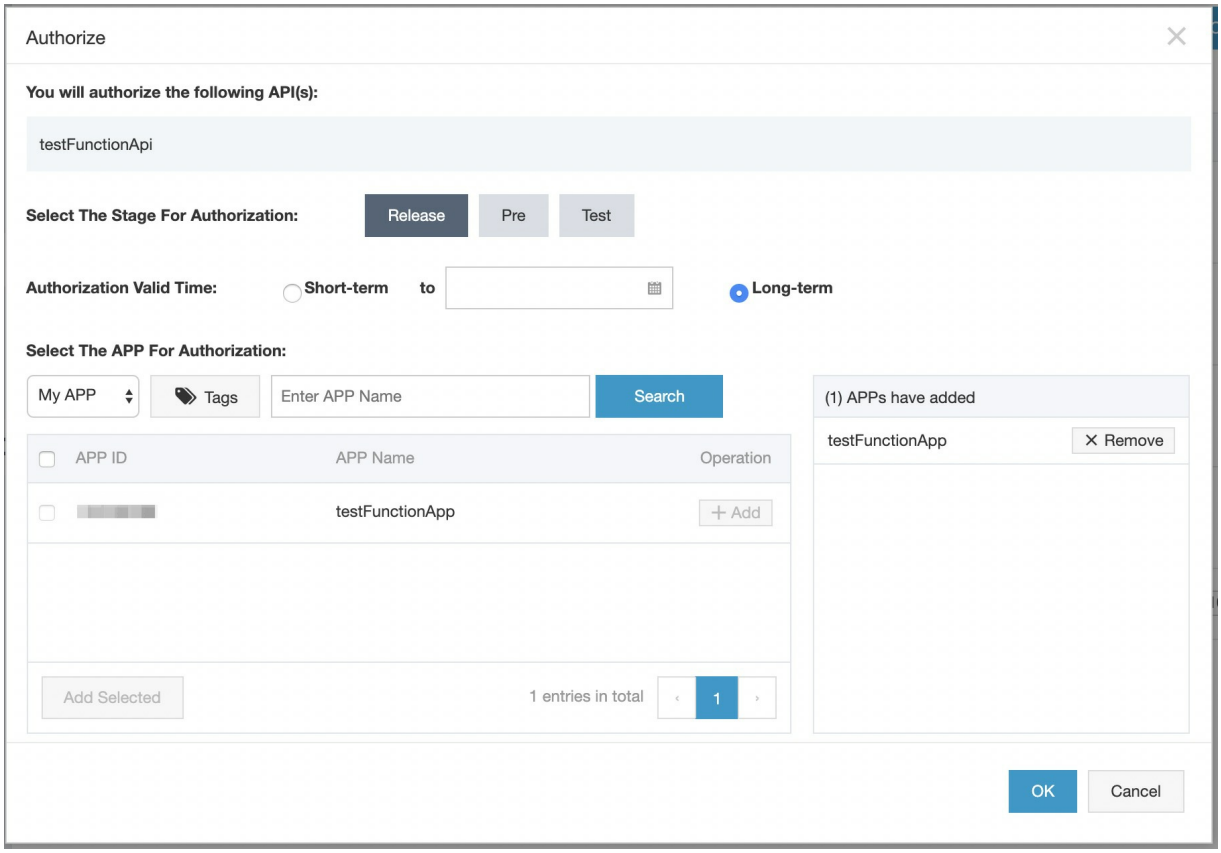
Step 10: Create an application

In the left-side navigation pane, choose `Consume APIs` > `APPs`. On the APP List page, click Create APP. As shown in the following figure, for an API operation whose Security Certification parameter is set to Alibaba Cloud APP, two authentication modes are provided for its applications: AppKey and AppCode. In this example, the AppCode mode is used to authenticate the application. For more information about the Alibaba Cloud APP authentication method, see Call an API operation by using an AppCode.



Step 11: Authorize the application

In the left-side navigation pane, choose Publish APIs > `APIs`. On the API List page, find the API operation you created and click `Authorize` in the Operation column. A dialog box appears, as shown in the following figure. Set the Select The Stage For Authorization parameter to the environment to which you have published the API operation. In this example, set this parameter to Release. Search for the application you created, click Add, and then click OK. A message appears to inform you that the application is authorized to call the API operation.



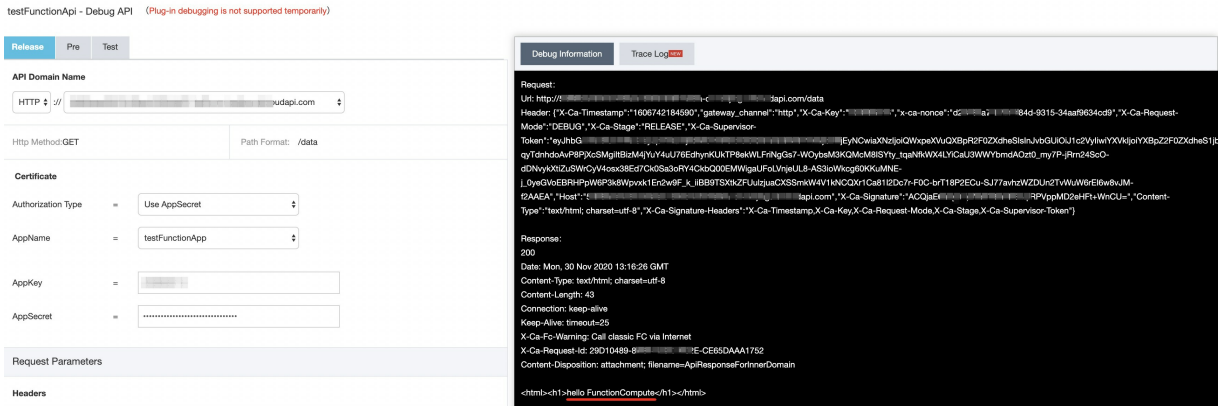
6. Debug the API operation

API Gateway supports online debugging. We recommend that you use this feature to check whether an API operation is correctly configured before you allow it to be called on clients.

Step 12: Debug the API operation

On the `API List` page, find the API operation you created and click `Debug` in the Operation column. A page appears, as shown in the following figure. If you have defined request parameters for the API operation, you can enter different values for the request parameters to check whether the API operation is correctly configured.

When you debug the API operation, make sure that the AppName parameter is set to an authorized application. The Stage parameter must be set to the environment where the application is authorized, otherwise the debugging may fail. In this example, set the Stage parameter to RELEASE.



The API response is the execution results of the function that you created in Function Compute. The following figure shows the code of the function.

index.js

```
'use strict';

var fs = require("fs")

exports.handler = function (event, context, callback) {

    console.log("request: " + JSON.stringify(event.toString()));
    // convert event to JSON object
    event = JSON.parse(event.toString());
    var query = event.queryParameters || {};
    var showResponse = query.response || 'html';

    switch (showResponse) {
    case "html":
        var htmlResponse = {
            isBase64Encoded: true,
            statusCode: 200,
            headers: {
                "Content-type": "text/html; charset=utf-8"
            },
            // base64 encode body so it can be safely returned as JSON value
            body: new Buffer("<html><h1>hello FunctionCompute</h1></html>").toString('base64')
        }
        callback(null, htmlResponse);
        break;
    case "json":
        var jsonResponse = {
            isBase64Encoded: true,
            statusCode: 200,
            headers: {
                "Content-type": "application/json"
            },
            // base64 encode body so it can be safely returned as JSON value
            body: new Buffer('{"hello": "FunctionCompute"}').toString('base64')
        }
        callback(null, jsonResponse);
```

7. Call the API operation

Now you have created the API operation and the application, authorized the application to call the API operation, debugged the API operation, and published the API operation to the online environment. In this step, you can call the API operation in your business system by using the AppCode.

Step 13: Call the API operation

For more information about how to call an API operation, see Call an API operation by using an AppCode. In this example, curl is used to call the API operation.

The following figure shows a sample response.

```
命令提示符
Microsoft Windows [版本 10.0.17763.1039]
(c) 2018 Microsoft Corporation。保留所有权利。

C:\Users\Administrator>curl -i -X POST "http://[redacted].alicloudapi.com/data?response=json" -H "Authorization:APPCODE [redacted]"
HTTP/1.1 200 OK
Date: Thu, 20 Feb 2020 06:35:02 GMT
Content-Type: application/json
Content-Length: 28
Connection: keep-alive
Keep-Alive: timeout=25
Server: Kaede/3.5.1.154 (sh001uvm2)
X-Ca-Request-Id: 01E29300-4F54-423C-8A74-D4E13ACC3A2D
Content-Disposition: attachment; filename=ApiResponseForInnerDomain

{"hello": "FunctionCompute"}
C:\Users\Administrator>
```

6.Access a domain name by using HTTPS

You can bind your domain name to an API Group hosted on API Gateway. API Gateway locates a unique API group by domain name and locates a unique API operation in the API group by using Path and HTTPMethod.

API Gateway provides a default Internet second-level domain name for each API group. A client can directly call the Internet second-level domain name up to 1,000 times per day. When you publish APIs in a production environment, you must bind an independent domain name to the target API group. The number of API calls is not limited for independent domain names.

An independent domain name that you want to bind to an API group must meet the following requirements:

- You must apply for an ICP filing or access the independent domain name at

  Alibaba Cloud ICP Filing.
- Before you bind the independent domain name to the target API group, you must add a CNAME record for the independent domain name to the second-level domain name of the group.
- The independent domain name has not been bound to an API group hosted on API Gateway by other users. If the independent domain name has been bound by other users, it must be verified when you attempt to bind it. If the API operations under the API group need to support HTTPS, you must import or upload an SSL certificate for the independent domain name.

1. Procedure for binding a domain name to an API group

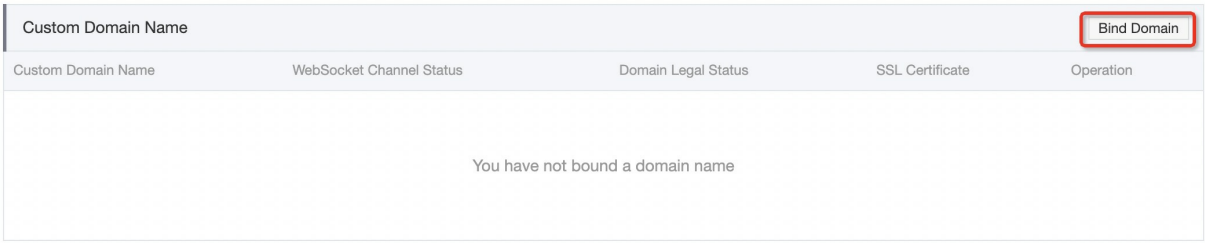
To bind your domain name to an API group hosted on API Gateway, follow these steps:

- Log on to the API Gateway console and bind your domain name to the target API group.
- Add a CNAME record for your domain name to the Internet second-level domain name provided by API Gateway to switch the traffic.

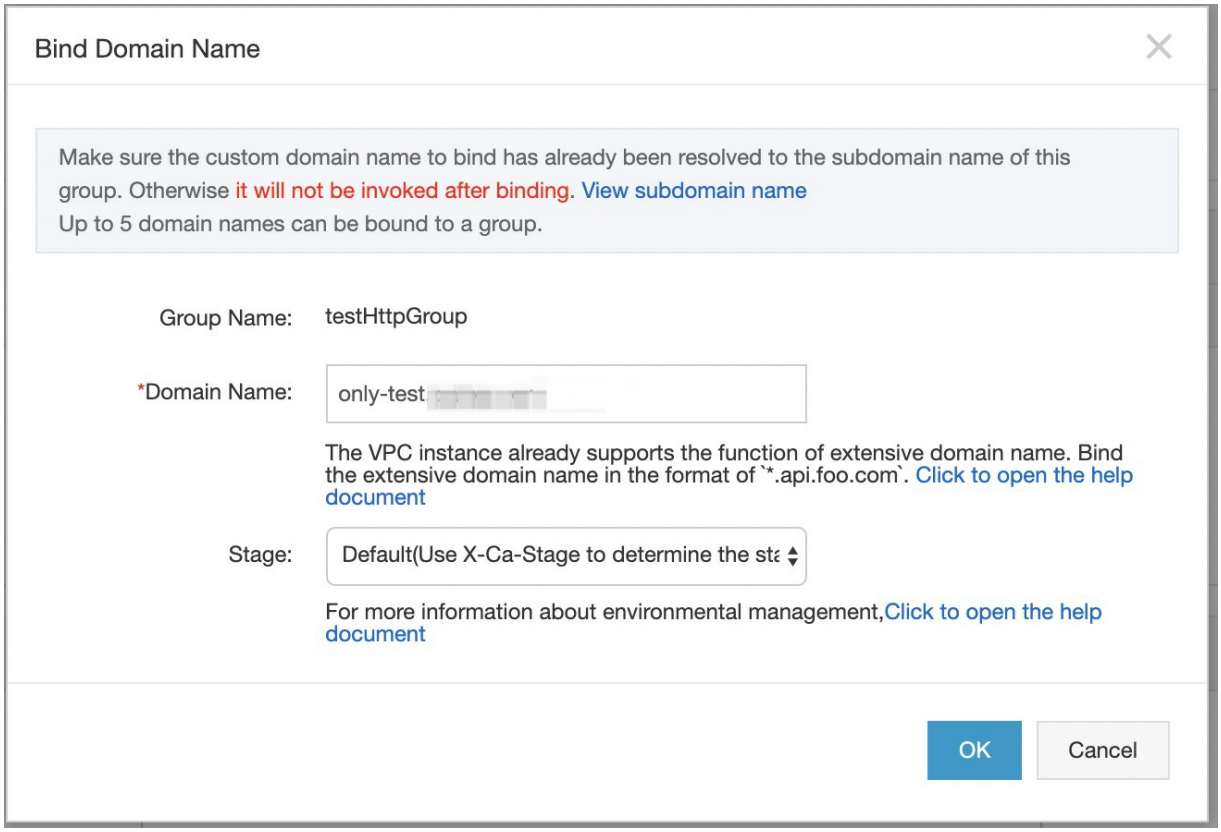
1.1 Bind a domain name to an API group

1. Log on to the API Gateway console. In the left-side navigation pane, click API Groups. On the page that appears, click the group to which you want to bind the domain name. The Group Details page appears.

2. In the lower-right part of the Group Details page, click Bind Domain.



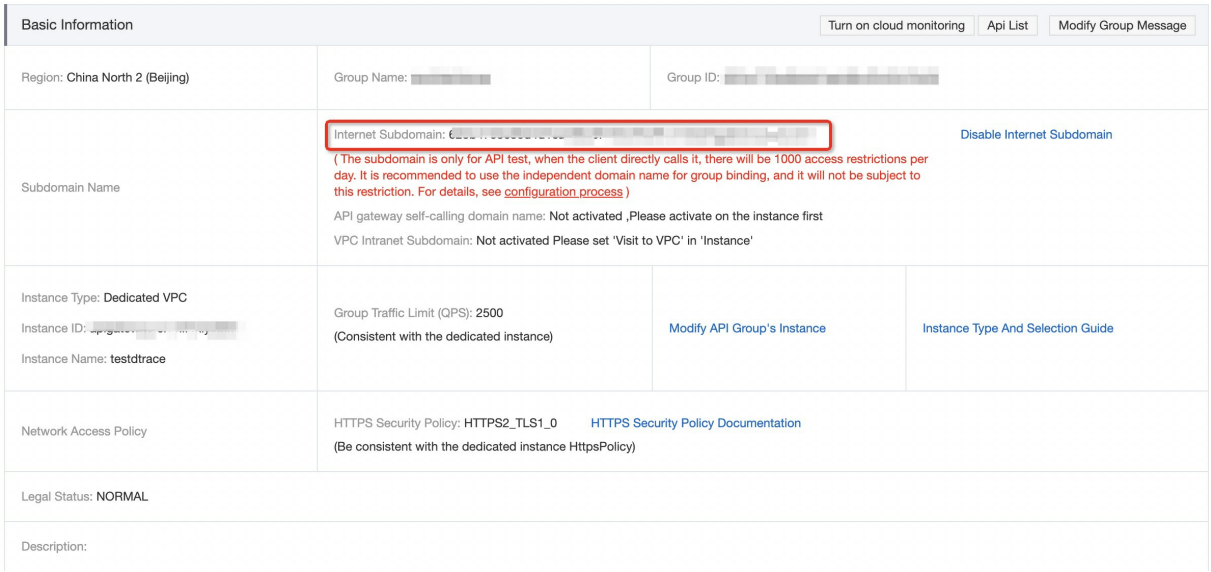
3. In the Bind Domain Name dialog box, enter your domain name and click OK.



1.2 Add a CNAME record for a domain name

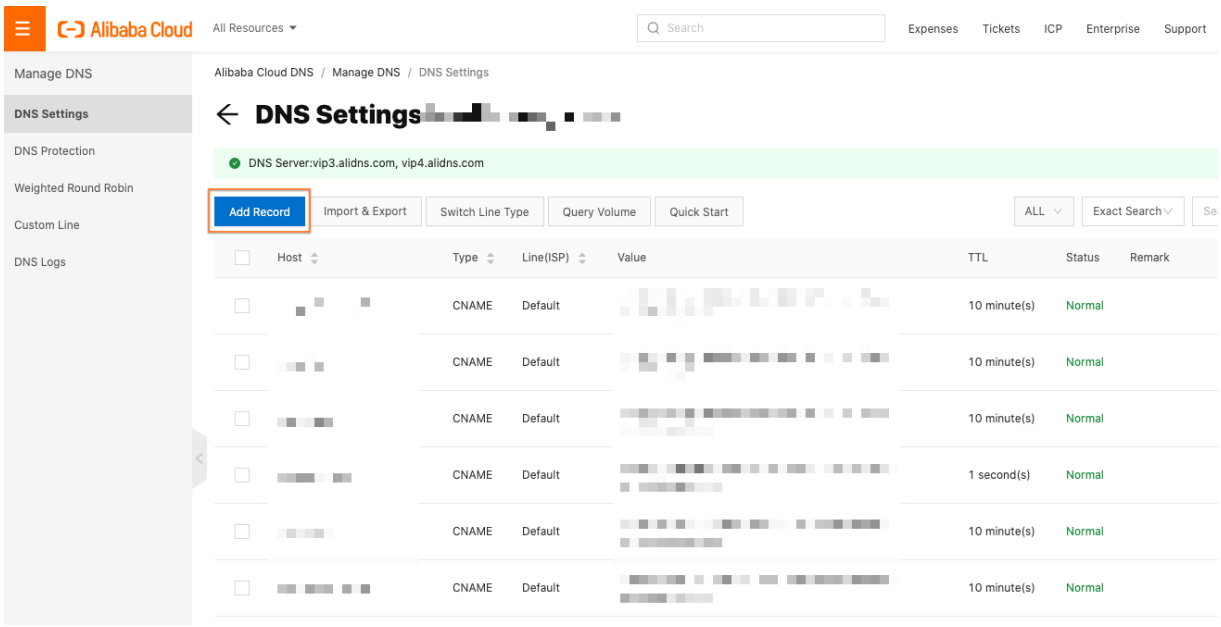
To add a CNAME record for your domain name to the Internet second-level domain name provided by API Gateway, follow these steps:

1. On the Group Details page, view Internet Subdomain of the group.

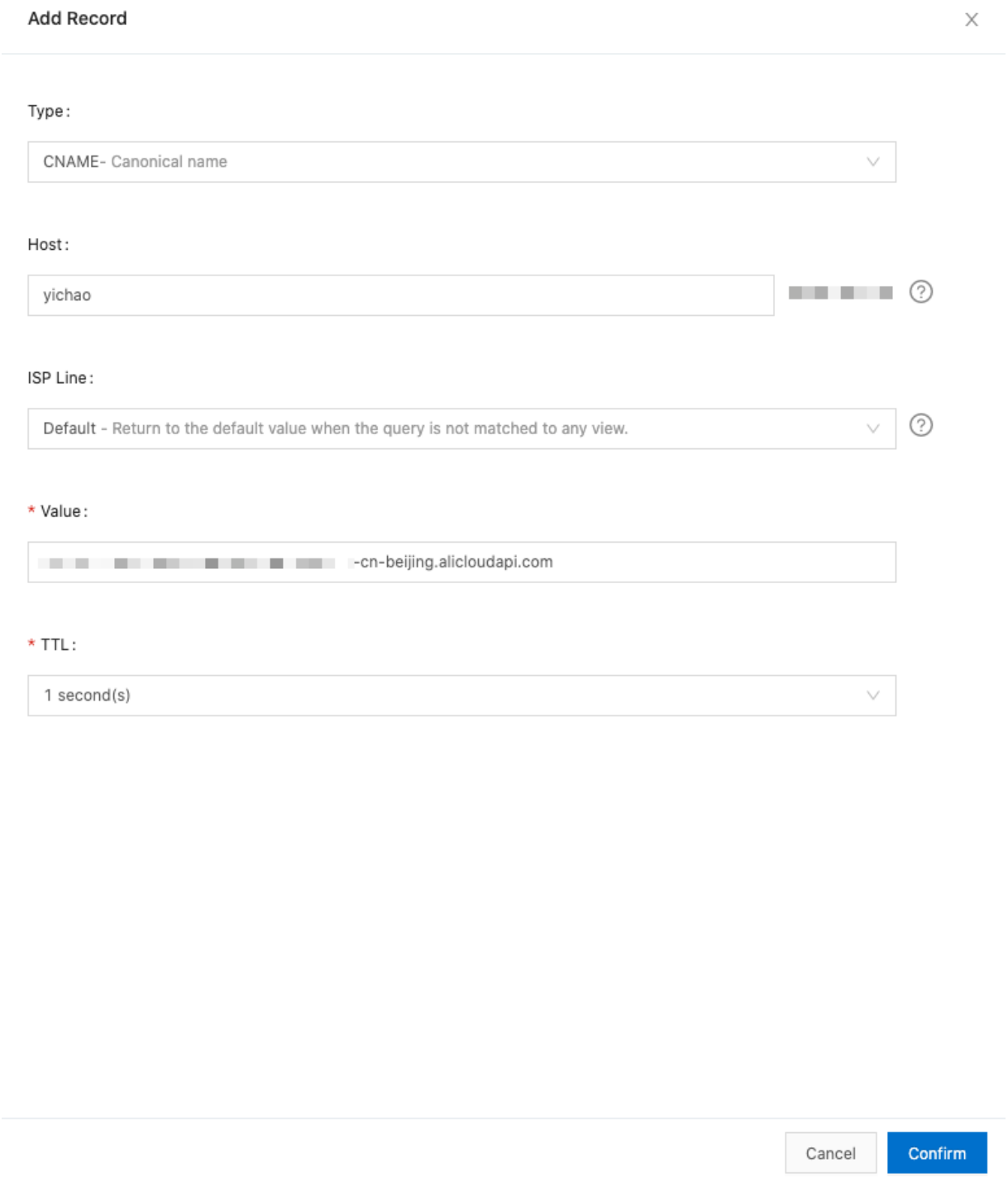


2. Log on to your DNS management platform. If you use Alibaba Cloud DNS, visit https://dns.console.aliyun.com. On the Manage DNS page of the Alibaba Cloud DNS console, click the target domain name to go to the DNS Settings page.

3. Add or modify a record for the domain name that you want to bind to the API group.



4. In the Add Record or Edit Record dialog box, set Type to CNAME and Value to the Internet second-level domain name that you obtained in step 2.



5. Click OK. After binding is complete, you can view the bound second-level domain name on the DNS Settings page.

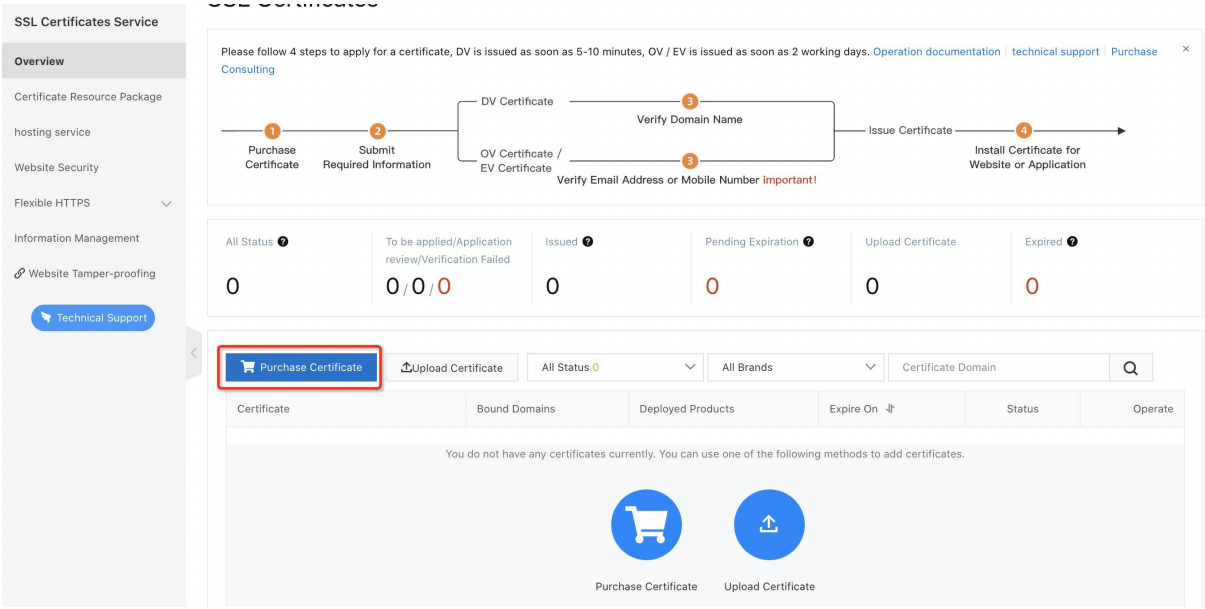
2. Procedure for uploading an SSL certificate for a domain name

After the binding is complete, you can use the bound domain name to call API operations under the API group in HTTP mode. If you want to call the API operations in HTTPS mode, you must upload an SSL certificate for the domain name. The certificate can be uploaded in either of the following ways: API Gateway automatically imports an SSL certificate from the Alibaba Cloud SSL Certificates Service or allows you to manually upload the SSL certificate that you obtained from other certificate service providers.

2.1 Generate an SSL certificate for a domain name

To generate a free SSL certificate by using the Alibaba Cloud SSL Certificates Service, follow these steps:

1. Log on to the Alibaba Cloud SSL Certificates console.



2. On the SSL Certificates page, click Purchase Certificate. On the page that appears, purchase an SSL certificate and bind your domain name to the certificate. For more information about how to purchase an SSL certificate, see Documentation of the Alibaba Cloud SSL Certificates Service. After you apply for an SSL certificate, go to the Group Details page of the target API group in the API Gateway console.

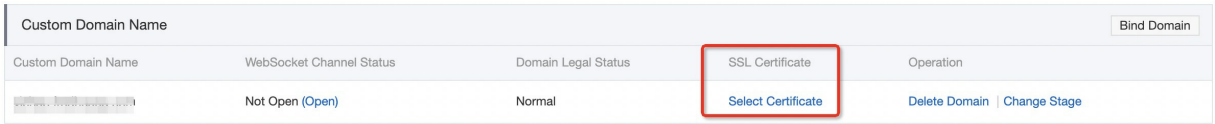
2.2 Import or upload the SSL certificate for the domain name

After you purchase or prepare a SSL certificate, import or upload the certificate for the domain name that you bound to the target API group in the API Gateway console. The following sections describe the certificate import and upload procedures.

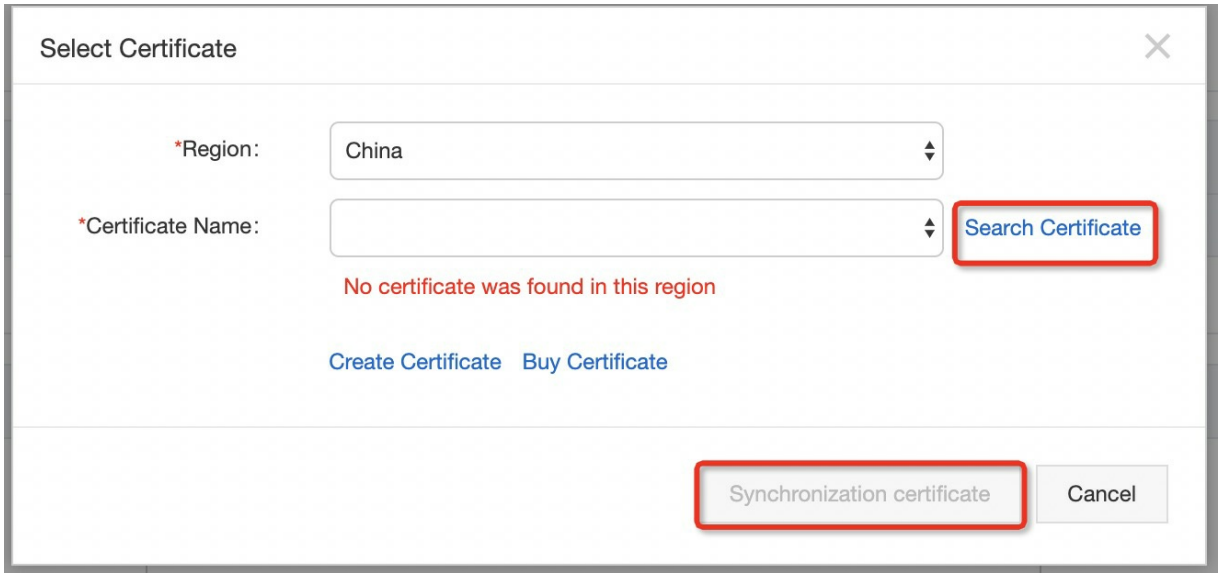
2.2.1 Import an SSL certificate

If you purchase a certificate by using the Alibaba Cloud SSL Certificates Service, follow these steps to import the certificate for the domain name that you bound to the target API group hosted on API Gateway:

1. Go to the Group Details page of the API Gateway console. In the list of bound domain names, find the target domain name and click Select Certificate in the SSL Certificate column.



2. In the Select Certificate dialog box, click Search Certificate. Then, select the required certificate from the search results and click Synchronization certificate.

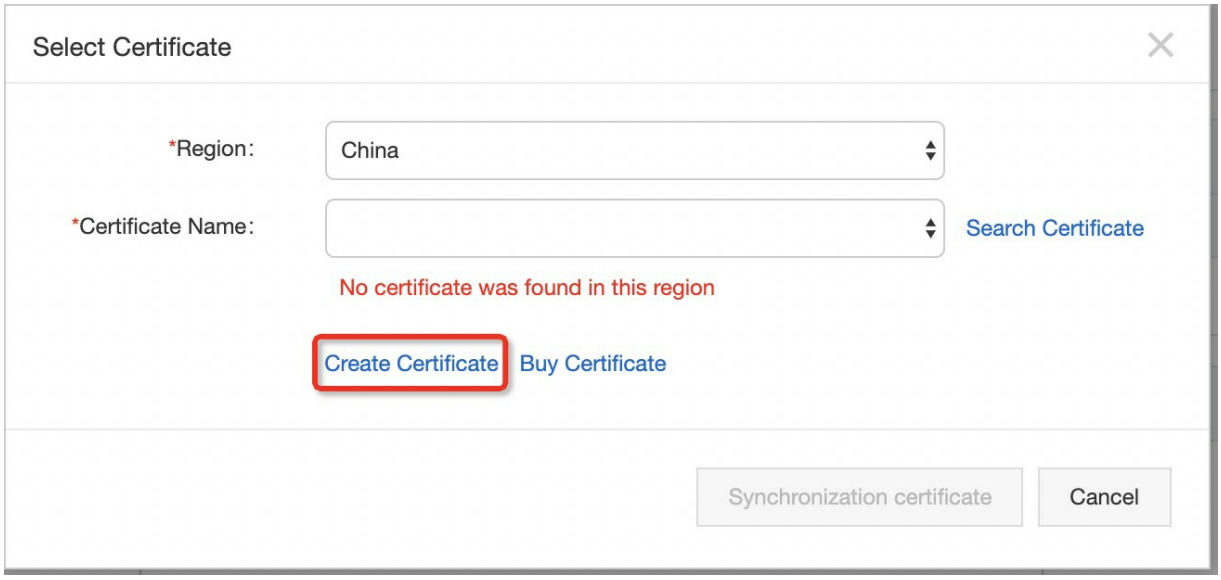


2.2.2 Upload an SSL certificate

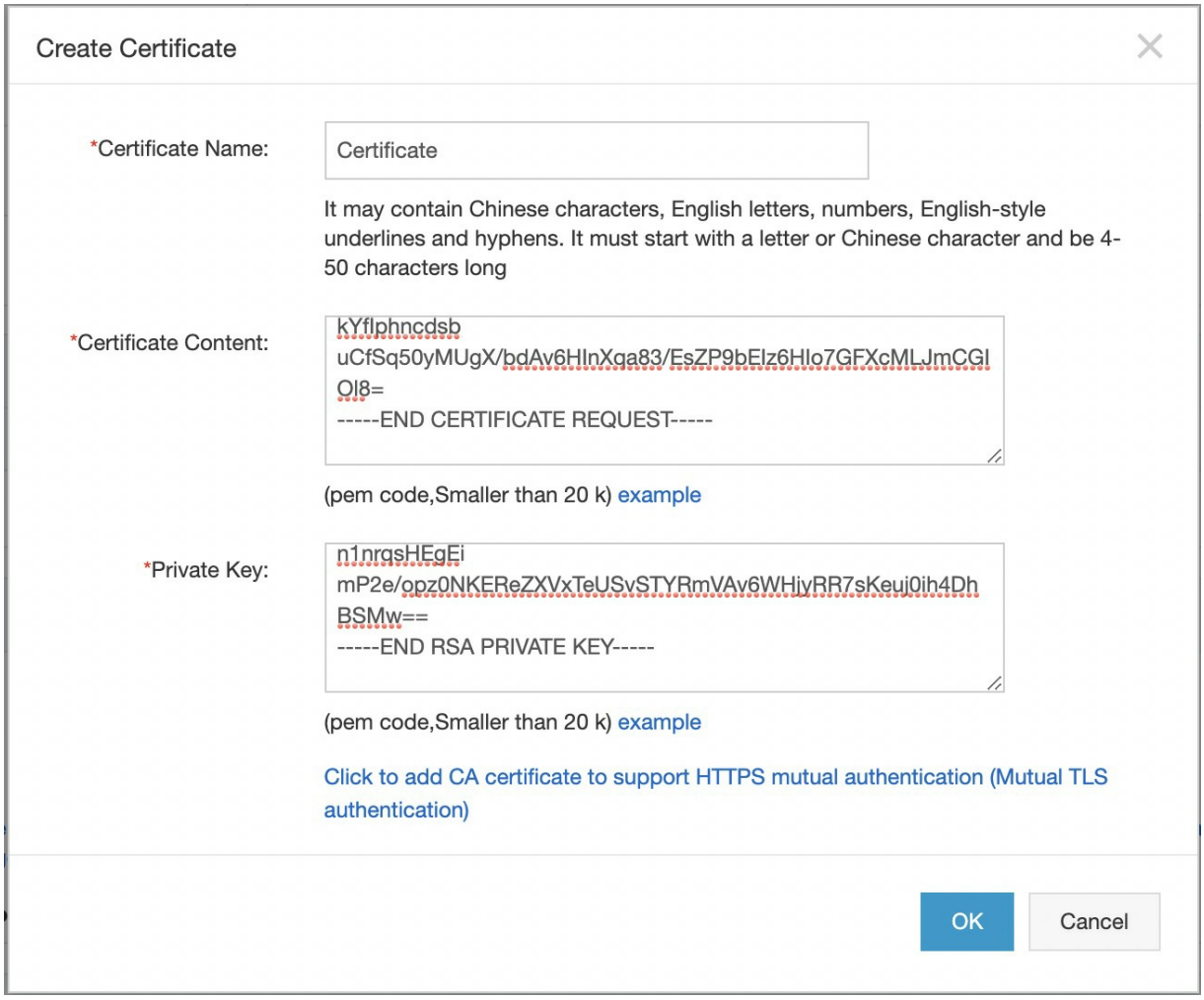
If your SSL certificate is not purchased from Alibaba Cloud, you can also upload your certificate to API Gateway. To upload the SSL certificate, follow these steps:

1. Go to the Group Details page of the API Gateway console. In the list of bound domain names, find the target domain name and click Select Certificate in the SSL Certificate column.

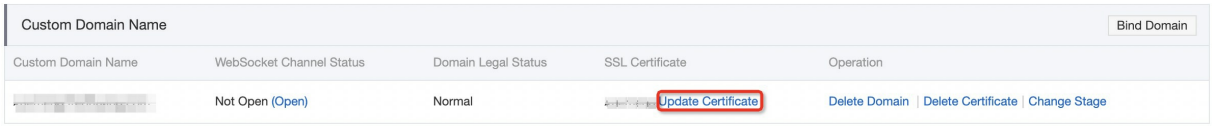
2. In the Select Certificate dialog box, click Create Certificate.



3. In the dialog box that appears, enter required information as prompted.



4. After the certificate is uploaded, go to the Group Details page. You can see that Select Certificate in the SSL Certificate column changes to Update Certificate.



After the certificate is uploaded, you can access the target domain name by using HTTPS.