API Gateway

Getting Started

Issue 03

Date 2025-01-16

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are the property of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei Cloud and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

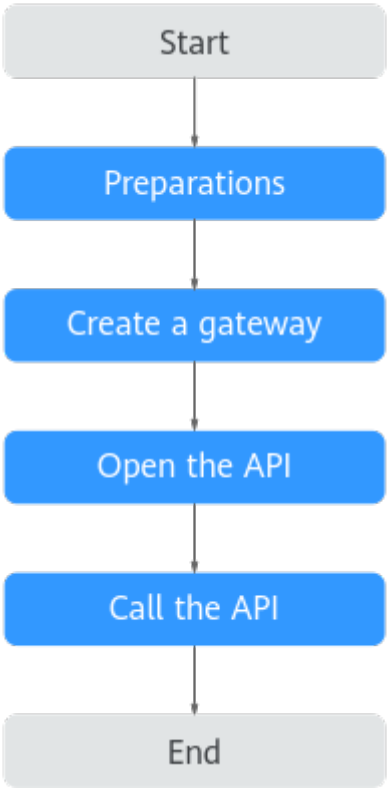
The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Contents

1 Quickly Opening and Calling APIs

This section describes how to quickly get started with APIG. The following uses **simple authentication** with an app as an example to describe how to quickly open and call APIs. **Simple authentication supports API calling only in HTTPS or gRPCS mode.**

Figure 1-1 Using APIG



1. **Preparations**

   Before using APIG, ensure you have configured a VPC, subnet, and security group.

2. **Create a gateway**

   Create a gateway with appropriate specifications.

3. **Open the API**

   Create an API that supports simple authentication with Mock backend. Debug the created API and publish it.

4. **Call the API**

   Create a credential and add an AppCode. Then use an API test tool to call the API with the AppCode.

Constraints

ELB load balancing is enabled by default after gateways are created in regions except **LA-Mexico City1** and **CN North-Beijing1**. Gateways with load balancing enabled do not support security groups. To disable access from specific IP addresses, see **access control policy**.

Step 1: Preparations

Step 1 Register with Huawei Cloud and complete real-name authentication.

If you already have a Huawei account, skip this step. If you do not have one, see **Signing up for a HUAWEI ID and Enabling Huawei Cloud Services** and **Real-Name Authentication**.

Step 2 Ensure that your account has sufficient balance before creating an APIG gateway.

To top up your account, see **Topping Up an Account**.

Step 3 Before creating an APIG gateway, ensure that your account has permissions to perform operations on APIG gateways.

- You must be assigned both the **APIG Administrator** and **VPC Administrator** roles so that you can create gateways.
- Alternatively, you must be attached the **APIG FullAccess** policy.
- To achieve fine-grained management of your cloud resources, create IAM user groups and users and grant specified permissions to the users. For details, see **Creating a User and Granting Permissions**.

Step 4 Before creating an APIG gateway, ensure that a VPC and a subnet are available.

Configure a VPC and subnet for the APIG gateway as required. You can use the current account's existing VPC and subnet or create new ones.

For details about how to create a VPC and a subnet, see **Creating a VPC**. **Note: The VPC must be created in the same region as the APIG gateway.**

Step 5 Before creating an APIG gateway, ensure that a security group is available.

Configure the security group for APIG gateways as required. You can use the current account's existing security groups, or create new ones. For details, see **Creating a Security Group**.

To connect to APIG gateways, add the security group rules described in **Table 1-1**. Other rules can be added based on site requirements.

Table 1-1 Security group rule

Direction	Protocol	Port	Source address	Description
Inbound	TCP	80/443	0.0.0.0/0	Intra-VPC Access

NOTE

- After a security group is created, it has a default inbound rule that allows communication among ECSs within the security group and a default outbound rule that allows all outbound traffic. If you access your APIG gateway using the private network within a VPC, you do not need to add the rules described in **Table 1-1**.
- ELB load balancing is enabled by default after gateways are created in regions except **LA-Mexico City1** and **CN North-Beijing1**. Gateways with load balancing enabled do not support security groups. To disable access from specific IP addresses, see **access control policy**.
- ELB functions as a load balancer for gateways, which support cross-VPC access. Gateways with public inbound access enabled are randomly assigned an EIP and cannot use an existing EIP.

----End

Step 2: Create a gateway

Step 1 Go to the **Buy Gateway page**.

Step 2 Configure the gateway according to the following table.

Table 1-2 Configuring the gateway

Parameter	Description
Billing Mode	Billing mode of the gateway. Select **Pay-per-use**.
Region	The region to which the gateway belongs. Select **CN-Hong Kong**.
AZ	The AZ of the gateway. Select **AZ1**, **AZ2**, and **AZ3**.
Gateway Name	Enter the gateway name, for example, **apig-test**.
Edition	Gateway specifications. Select **Basic**.
Scheduled Maintenance	The period for gateway maintenance. Retain the default value.
Enterprise Project	Select **default**.
VPC	Select the prepared VPC and subnet.
Public Inbound Access	Allows external services to call instance creation APIs using EIPs. Enable the public network entry.
Security Group	Select the prepared security group.

Step 3 Click **Next**.

Step 4 Confirm the configuration, read and confirm your acceptance of the service agreement, and click **Pay Now**.

----End

Step 3: Open the API

Step 1 Create an API.

1. In the navigation pane, choose **API Management** > **APIs**.
2. Click **Create API** > **Create API** and configure the frontend.

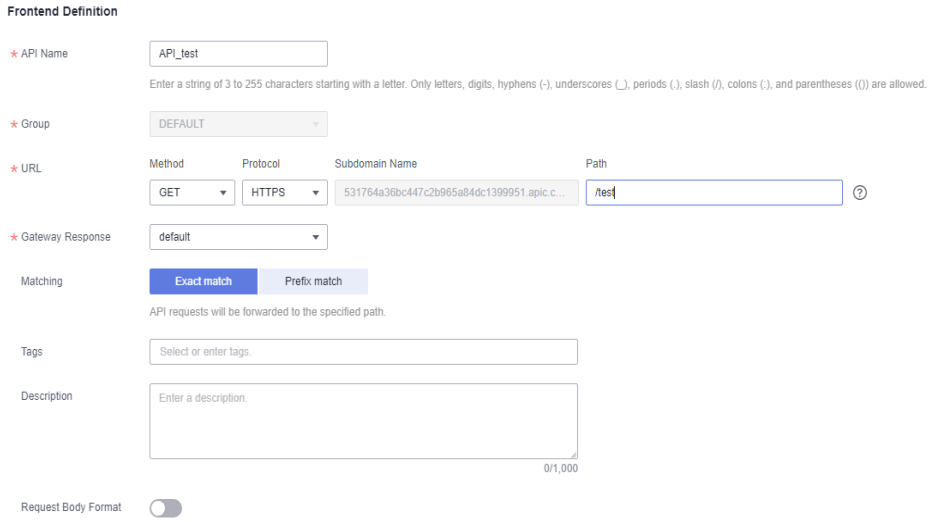


Table 1-3 Frontend definition

Parameter	Description
API Name	Enter the API name, for example, **API_test**.
Group	Select the default group **DEFAULT**. To create a group, click **Create API Group**. For details about how to create an API, see **Creating an API Group**.
URL	**Method**: Request method of the API. Set this parameter to **GET**. **Protocol**: Set this parameter to **HTTPS**. **Subdomain Name**: The subdomain automatically allocated to the API group. The subdomain name of the **default** API group is used. Path: path of the API request. Set this parameter to **/test**.
Gateway Response	The response to be displayed if APIG fails to process an API request. Default: **default**.

3. Configure security settings based on the following table.

Table 1-4 API request definition

Parameter	Description
Authentication Mode	API authentication mode. Set this parameter to **App**.
Simple Authentication	If you enable this option, API Gateway verifies only the AppCode and the request signature does not need to be verified. For this example, enable **Simple Authentication**.

4. Click **Next** and configure the default backend information.

Table 1-5 Parameters for defining a Mock backend service

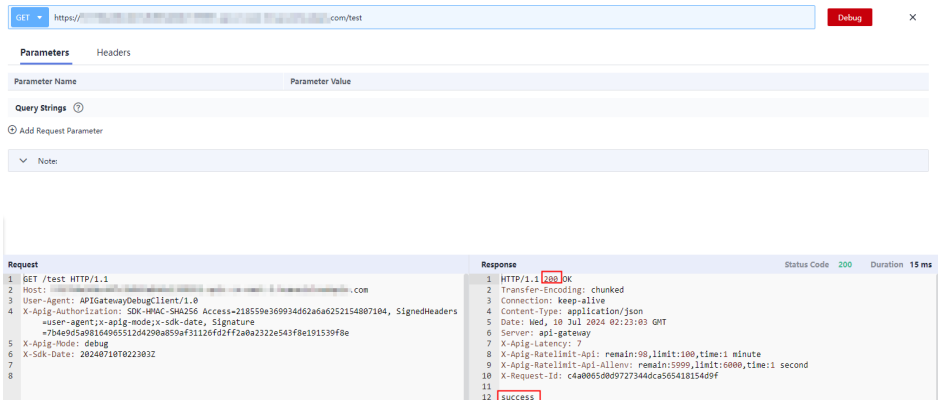
Parameter	Description
Backend Type	Backend service type. Select **Mock** to prevent API requests from being forwarded to the backend service. This is useful if you need to debug APIs when the backend is unavailable. If a backend service is available, configure other backend service types as required. For details, see **Creating an API**.
Status Code	The HTTP status code returned by the API. Use the default **200** here.
Response	Expected result to the API caller for debugging and verification. Enter **success** here.

5. Click **Finish**.

Step 2 Debug the API.

1. On the **APIs** tab page, select an API and click **Debug**.
2. Click **Debug** on the right of the URL. The API request and response information are displayed at the bottom of the page.

   If the API is successfully called, the status code **200** is displayed, and **success** is returned for the Mock backend. Otherwise, rectify the fault by referring to **Error Codes**.



Step 3 Publish the API.

1. On the **APIs** tab, click **Publish Latest Version**.
2. Select the environment in which the API is to be published. Choose the default environment **RELEASE**. Or you can click **Create Environment** to create an environment. For details, see **(Optional) Configuring the Environment and Environment Variables**.
3. Click **OK**.

----End

Step 4: Call the API

Step 1 Create a credential.

1. In the navigation pane, choose **API Management** > **Credentials**.
2. Click **Create Credential** and enter the credential name. In this example, enter **apptest**.
3. Click **OK**.

Step 2 Bind the credential to the API. **Note that only APIs that use app authentication can be bound.**

1. In the **Operation** column of the created credential, click **Bind to APIs**.
2. Select an environment, API group, and APIs.
3. Click **OK**.

Step 3 Add an AppCode.

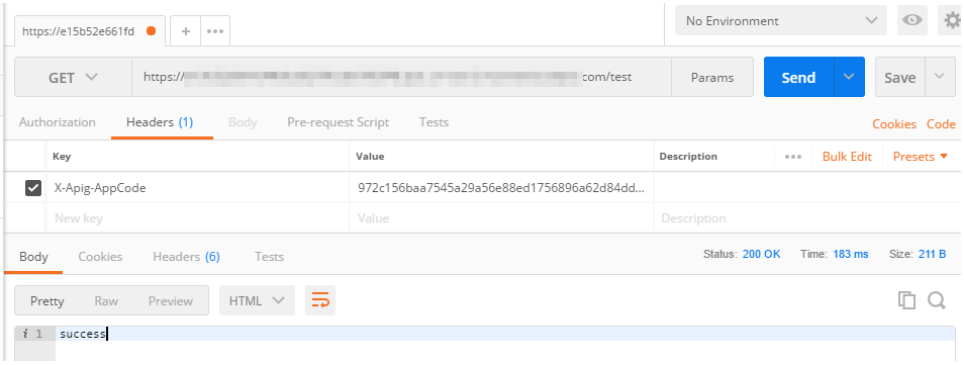
1. In the credential list, click the created credential to go to the credential details page.
2. Under **AppCodes**, click **Add AppCode**.
3. Select **Automatically generated**.
4. Click **OK**.

Step 4 Call the API.

Use the API test tool to configure the API request and authentication.

1. Select **GET** as the request method. On the **APIs** page, copy the URL in the format of **https://*debugging domain name*/*path*** to the API test tool.
2. Add the header parameter **X-Apig-AppCode** and set the parameter value to the generated AppCode.
3. Send the request.

   If the API is successfully called, the status code **200** is displayed, and **success** is returned for the Mock backend. Otherwise, rectify the fault by referring to **Error Codes**.



----End

Related Documents

- For details about how to create an API, see **Creating an API**.
- For more information about API calling, see **Calling an API**.
- If an API fails to be called, refer to **Error Codes**.
- VPC owners can share the subnet in the VPC with one or multiple accounts through Resource Access Manager (RAM). Through VPC sharing, you can easily configure, operate, and manage multiple accounts' resources at low costs. For more information about VPC subnet sharing, see **VPC Sharing Overview**.

2 Getting Started with Common Practices

You can use the common practices provided by APIG to meet your service requirements.

Table 2-1 Common practices

Practice	Description
Developing a Custom Authorizer with FunctionGraph	In addition to IAM and app authentication, APIG also supports custom authentication with your own authentication system, which can better adapt to your business capabilities. Custom authentication is implemented using the FunctionGraph service. You can create a FunctionGraph function so that APIG can invoke it to authenticate requests for your API.

Practice	Description
Request Throttling 2.0	If the number of requests initiated from public networks for open APIs on APIG is not limited, the continuous increase in users will deteriorate the backend performance. And what's worse, the website or program will break down due to a large number of requests sent by malicious users. The traditional request throttling policies of APIG throttle requests by API, user, credential, and source IP address. However, as users and their demands become more diversified, these traditional policies cannot meet the requirements for more refined rate limiting. To resolve this issue, APIG has launched request throttling 2.0, which is a type of plug-in policy. The 2.0 policies enable you to configure more refined throttling, for example, to throttle requests based on a certain request parameter or tenant.

