API Gateway

Quick Start for Consumers

Quick Start for Consumers

This article guides you through the process of calling the API services published by other providers. You must follow these steps:

1. Obtain API documentations.
2. Create an app.
3. Obtain authorization.
4. Call an API.

Three elements of calling an API

Three basic conditions are required to call an API:

- API: The API you are going to call, you must obtain detailed parameter definitions.
- App: The app is your identity when calling the API. AppKey and AppSecret are used for authentication.
- Permission between API and app: The app must be authorized to call the API. This permission can be set up through the authorization function.

The following articles provide the details about how to meet the three conditions and show a Demo of calling an API.

Authorized by the provider

You must create an app and share the AppId with the provider so they can authorize your app. This article assumes that you have completed the authorization process.

Go to the **App Management** page on the API Gateway console and view the created apps.

Click the app name to go to the detail page. You can see the basic information of the app and the most important content, **AppKey** and **Authorized API**.

Authorized API shows the APIs that the app is authorized to call. Click **Detail** for more information.

An app is your identity to call an API. The identity and permission verification during API calling is specific to apps. In the API Gateway, calling an API requires authorization, which is also granted to the corresponding app.

When creating an app, you must specify a unique name for the app under your account.

After an app is created, the system assigns the app an AppKey and AppSecret which are encrypted as the signature information. Your request must include the signature information. Based on this, the gateway verifies your identity. For more information of apps, see App.

Authorization grants an app the permission to call an API. Your app needs authorization for an API before calling it. At the public beta stage, the API service provider establishes or revokes permissions.

You must provide the API service provider with your AppID or Alibaba Mail account to find and authorize your app. After authorization, you can see the authorized API under the app on the console.

Based on the SDKs provided by the API Gateway, you can write codes to call an API. API Gateway provides SDKs of the mainstream languages for the Web client and mobile client and continuously provides SDKs of more language types. You can also edit an HTTP request to call an API.

Through the preceding steps, you can obtain the domain name, path, and parameter description from the service provider. The created app is used as your requester identity. The AppKey and AppSecret are used for calculating the encrypted signature. The demo link for signature calculation is as follows:

After your app has been authorized, you can call the API. The API request structure is as follows:

//If the service address is a13db7999e494a90819cce500130034d.com.

//If the path is /web/cloudapi/mapping/service.

//If the query content is a=name, b=12.

//Then the URL of the request is as follows:

```
http://a13db7999e494a90819cce500130034d.com/web/cloudapi/mapping/service&pound;&iquest;a=name&b=12
```

//Requesting method.

```
POST  HttpMethod: POST
```

//Headers must include signature information and certain parameters.

```
X-Ca-Version:  1      //API version
X-Ca-Signature-Headers: X-Ca-Version,X-Ca-Key,X-Ca-Stage,X-Ca-Timestamp //Headers involved in signature calculation
X-Ca-Key: 60028305 //AppKey
X-Ca-Stage: test //Stage
```

```
X-Ca-Timestamp: 1456905123049 //Time stamp
X-Ca-Signature: UAaH/qteir4G9UK4YR+NWdyq+c1rjl0PvtO/C1Qo68U= //Signature
```

//Standard HTTP header.

```
Host:  a13db7999e494a90819cce500130034d.com         //Service address
Date: Wed 02 Mar 2016 07:52:02 GMT
User-Agent: Apache-HttpClient/4.1.2 (java 1.6)
Content-Type: application/x-www-form-urlencoded; charset=utf-8
```

//Body content.

```
Amount=11&InstanceId=ClientInstanceId&InstanceName=ClientInstanceName
```

When you call an API, either the HTTP or HTTPS request must include signature information. The AppKey indicates your identity. The AppSecret is the key used to encrypt the signature string and verify the signature string on the server. For more information about the methods of calculating and passing the encrypted signature, see Portal and Protocol.

For more information, see User Manual (Call an API).