API Gateway

Quick Start for Providers

Quick Start for Providers

This document introduces how to create and enable an API. To enable an API, follow the steps below:

1. Create an API group.
2. Bind a domain.
3. Create an API.
4. Publish the API.
5. Authorize the API.

An API group is a management unit of APIs, and needs to be created before creating an API.

An API group has a corresponding region. Once an API group is selected, the region is determined and cannot be changed.

A unique second-level domain name is bound to the created group. You can access the second-level domain name to call APIs under test in the group.

To enable an API, you need to bind an independent domain name to the group. The independent domain name needs to be filed on the Alibaba Cloud system, and its CNAME will be resolved to the group’ s second-level domain name. You can access the independent domain name to call online APIs in the group.

If your API supports the HTTPS protocol, you need to upload the SSL certificate of the independent domain name.

A domain name is bound to an API group. API Gateway uses the domain name to locate a unique API group, and locate the unique API through Path+HTTPMethod.

To enable an API, you need to bind an independent domain name to the API group. The independent domain name must conform to the following requirements:

1. The independent domain name needs to be filed on the Alibaba Cloud system, and then the request can arrive at your backend services.
2. If the domain name is filed on another system, the system needs to be connected to the Alibaba Cloud system before the domain name can be used. For more details, refer to Filing and Connection Process.
3. You need to resolve the CNAME of the independent domain name to the group’ s second-level domain name, and then bind the independent domain name to the group. Otherwise, the system returns an error during the binding operation.
4. Domain names need to be verified within one day. Any binding requests not processed

within one day will be automatically withdrawn by the system.
5. To bind an independent domain name of another group to the current group, resolve the independent domain name and then bind it to the current group.

The domain name can be bound after it is filed and its CNAME is resolved. For more details about filing or connection, refer to [Filing and Connection Process].

If the API in the group supports the HTTPS protocol, you need to complete the SSL certificate information for the independent domain name. The certificate file cannot be uploaded. You need to input the certificate name, content, and private key.

You can create an API after creating an API group. API creation is a process defining an API request. The following parameters must be defined in sequence:

1. Basic API information: Group, name, type, and description. Once the API group is selected, the region is determined and cannot be changed.
2. Information of API backend services: Type, address, and timeout time of backend services. The service address may contain dynamic parameters which are included in the path. Parameters in the service address can only be accepted from the path.
3. API request format: Protocol, method, path, parameters (including headers, query, body, constant parameters, and system parameters), parameter mapping, and parameter verification. Note that the parameter names, including backend parameter names, cannot be repeated.
4. API returned results: Type and example of returned results. The gateway does not process returned results.

Once all parameters are defined, an API is created and is ready to be enabled. For more details, refer to User Manual (Enable an API).

After creating an API, you can publish it for testing. Create an app and access a second-level domain name to call the API to be tested. For how to call an API, refer to User Manual (Call an API).

You can publish an API to production after it is bound to an independent domain name. After you authorize your customer’ s app to access the API, your customer can access the independent domain name to call your API in the production environment.

You can use the API Gateway to manage the API version in the test or production environment. You can publish the app, remove the app, or switch the API version. Version switching takes effect in real time.

An app indicates the identity of the requester. Each app has an AppKey and AppSecret which are used for calculating the encrypted signature. The gateway verifies the identity of the requester.

Whether you or your customers attempt to test or call an API, an app needs to be created as the identity of the requester, and permission needs to be authenticated to the app. The authorization

operation is as follows:

1. Obtain the AppID of the app to be authorized or the Alibaba Mail account of the app owner.
2. On the authorization operation page, select one or more APIs for which call permissions are to be made available, and click **Test/Production**.
3. Use the AppID or Alibaba Mail account to search the app.
4. Confirm the authorization.

Now, you have created and enabled an API which can be called by your customer. When a request arrives at the gateway, the gateway verifies the app' s identity and permissions. You can configure security protection for your API, for example, configuring a traffic control policy to limit the access traffic. The gateway also supports a signature of the backend services. You can set a signature key for authentication when the gateway sends requests to your backend.

Now, you can configure security protection. API Gateway supports two security measures: backend signature and traffic control policy.

The signature key is used for your backend authentication. After the API is bound to a signature key, the request sent by the gateway to your backend carries the signature information. You can perform signature verification on the request at the backend through symmetric encryption. For details about adding a signature to the HTTP service, refer to Backend HTTP Service Signature.

The traffic control policy is used to control the API traffic. When a traffic control policy is configured for the API, the gateway controls the traffic per minute, hour, or day for APIs, users, and apps.

You can perform more API lifecycle management operations on the console, for example, API deprecation, API version switching, and API call monitoring and warning. For more details, refer to User Manual (Enable an API).