API Gateway

Product Introduction

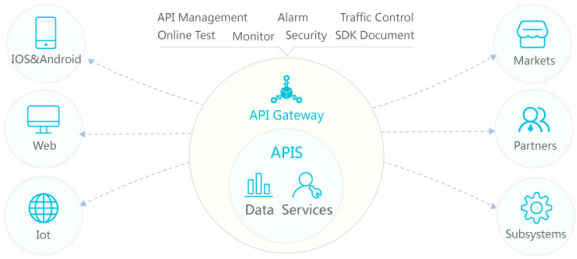
Product Introduction

What is API Gateway

API Gateway provides you with a complete API hosting service, helping you open capabilities, services, and data to your partners in the form of APIs. You can also release your APIs on the API marketplace for other developers to purchase.

- This service provides multiple techniques, including attack defenses, anti-replay, request encryption, identity authentication, permission management, and throttling to guarantee API security and reduce the risk of opening APIs.
- This service provides a full range of lifecycle management functions, including API definition, testing, release, and removal, generates SDKs and API instructions, and increases the efficiency of API management and iteration.
- The service provides convenient O&M tools, such as monitoring, alarms, analysis, and the API marketplace, reducing API operation and maintenance costs.

API Gateway maximizes capability multiplexing, so enterprises can share capabilities and focus more on strengthening and advancing their own business.



Benefits

Increases productivity

API Gateway provides a routine maintenance service for API documentation, SDK management, API

version management, and other relevant scenarios. This removes the hassle of API management and significantly reduces maintenance costs.

Only pay for actual services

API Gateway supports activation, routine API management, document generation, SDK generation, throttling, and permission control for free. You only need to pay for actual API calls.

Large scale and high performance

API Gateway is deployed in a distributed way. It can perform automatic scaling, handle massive API access requests, and guarantee low delay to provide highly secure and efficient gateway functions for your backend services.

Secure and stable

You only need to open your service to API Gateway on the intranet, without worrying about security issues. API Gateway provides strict permission management, precise throttling, and comprehensive alarms, and precise monitoring functions, guaranteeing that your service is secure, stable, and controllable.

Features

API Gateway provides the following features:

API lifecycle management

- A range of lifecycle management functions, including API release, API testing, and API removal are supported.
- Routine maintenance functions such as API management, API version management, quick API rollback and more are supported.

Comprehensive security protection

- Multiple authentication methods, and HMAC (SHA-1, SHA-256) algorithms for signatures are supported.
- HTTPS protocol and SSL encryption are supported.
- Active mechanisms such as anti-attack, anti-injection, anti-request replay, and anti-request tampering are supported.

Flexible permission control

- Users can use apps as the identity for API request, and the gateway supports app-based permission control.
- Only authorized apps can send requests to the API.
- API providers can authorize an app to call an API.
- If an API is available on the API marketplace, buyers can grant their own apps with the purchased API.

Precise throttling

- Throttling can be used to control API access frequency, app request frequency and user request frequency.
- Throttling can be measured in minutes, hours, or days.
- The gateway also supports throttling exceptions, allowing you to set special apps and users.

Request verification

- API Gateway supports parameter type and parameter value (range, enumeration, regular expression) verification. Invalid parameter types and values result in immediate rejection by the API gateway. This minimizes waste of backend resources on invalid requests and significantly reduces backend service processing costs.

Data conversion

- By configuring mapping rules, data between the frontend and backend can be translated. Front end requests and returned results can be converted through API Gateway.

Monitoring and alarms

- API Gateway provides visualized API monitoring in real time, including call volume, traffic volume, response times, error rates, and successively added dimensions.
- Historical data querying and the facilitation of overall analysis is supported.
- You can also configure warning methods (notifications sent through SMS or email) and subscribe to warning notifications to stay informed about your API operational status in real time.

Automated tools

- API Gateway automatically generates API documentation which can be viewed online.
- API Gateway provides demo SDKs in multiple languages for better accessibility and helping to reduce O&M costs.
- API Gateway provides visualized debugging tools for rapid testing and release.

API marketplace

- You can release APIs on the API marketplace for other developers to purchase and use.

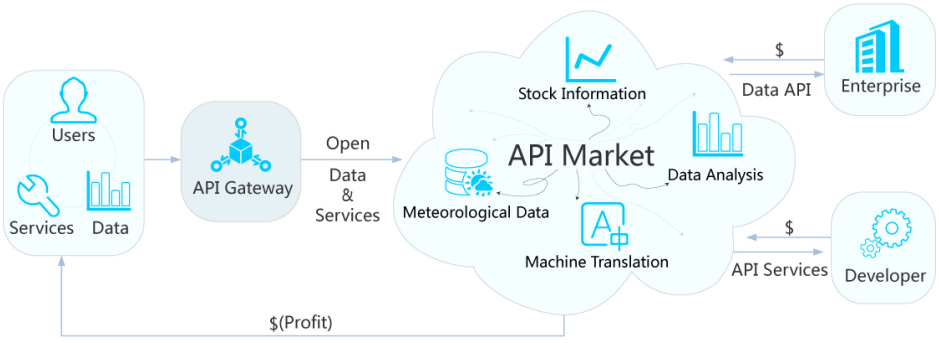
Scenarios

API Gateway allows you to provide APIs for a variety of scenarios. With API Gateway, you can open APIs to partners and developers to monetize your enterprise’ s core capabilities and establish an API ecosystem. You can adapt your APIs to multiple terminals (such as mobile and Internet devices) and separate the frontend and backend of the system. Furthermore you can create completely modular, micro-service-based systems.

1. Establish an ecosystem for capability sharing and coordinated development

As user numbers grow, and user needs diversify, enterprises must explore new business models to solve various scenario-specific problems for their customers. With API Gateway, standard API services are provided that allow other developers to integrate some or all APIs into their own apps. This opens up new services, help enterprises establish new business ecosystems, and promote cross-sector innovation.

- Using API Gateway, you can share your core capabilities with your partners to realize deep cooperation and synergetic development.
- By releasing APIs on the Alibaba Cloud marketplace, you can provide capabilities, services, and data to a wide range of developers for purchase and use.
- On the API marketplace, you can purchase sophisticated capabilities and services from third parties to avoid tiled exploration, focus on service specialty, and boost service development.

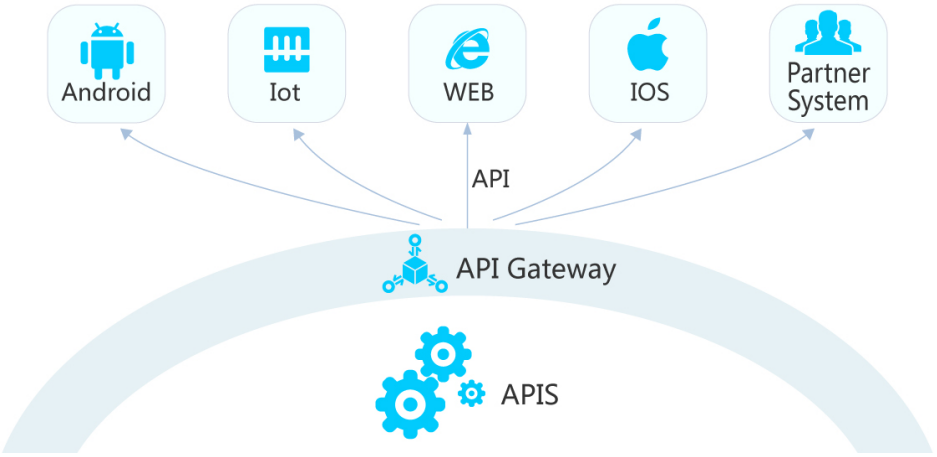


2. Secure implementation of multi-terminal unification for a single service with multi-terminal output

As mobile and IoT devices become increasingly common, APIs are now required to support more types of terminal devices to expand business scale, which also increases system complexity. Using API Gateway, you can adapt your APIs to multiple terminals by adjusting the API definition in API

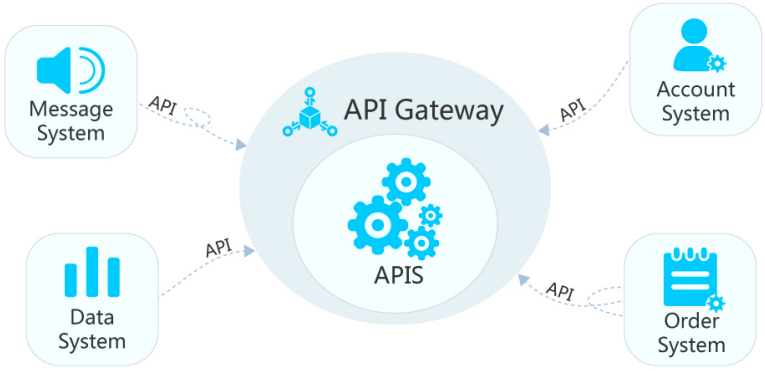
Gateway without additional configurations needed.

- You only need to maintain a single service system that can provide output to multiple terminals. By adjusting the API definition, you can support apps, devices, web terminals, and various other terminals.
- You do not need specialized APIs for different scenarios, significantly reducing management and O&M costs.



3. Easy system integration and standardization

- With API Gateway, you can standardize your own inter-system interfaces and apply pre-standardized interfaces for system integration.
- You can quickly integrate and manage resources, minimizing resource waste and operation redundancies while focusing on channeling resources for business development.



Glossary

Before using API Gateway, we recommend that you familiarize yourself with the following terms.

Term	Explanation
App	A user needs to create an app as the identity to call an API.
AppKey, AppSecret	Each app has a key pair, which is encrypted as signature information in the request.
Encrypted signature	An API request carries secure signature information, based on which API Gateway verifies the requester’ s identity.
Authorization	The API service provider grants an app permission to call an API. Only authorized apps can call APIs.
API lifecycle	The API service provider manages an API in stages, including API creation, testing, release, deprecation, and version switching.
API definition	When creating an API, the API service provider has to set rules for the API such as backend service, request format, received format, and returned format.
Parameter mapping	When the parameters in a user’ s request are inconsistent from those at the API backend, the API service provider can configure parameter mapping.
Parameter verification	The API service provider sets verification rules for input parameters. Based on such rules, API Gateway filters invalid requests.
Constant parameters	You do not must input such parameters, however, the backend service must always receive them.
System parameters	You can configure the gateway to include certain system parameters such as CaClientIP (request IP address) into the request sent to your backend.
API group	The API service provider manages APIs through the group. Before creating an API, you first must create a group.
Second-level domain name	When creating a group, the system binds the group with a second-level domain name for testing API calls.
Independent domain name	When opening an API, you must bind an independent domain name to the group. Customers must access the independent domain name to call the API.
Signature key	The API service provider can create a

	signature key and bind it to the API. When sending a request to the service provider’ s backend, the gateway carries the signature information for backend security verification.
Throttling policy	The API service provider uses a throttling policy to control the traffic of APIs, users, and apps at the minute, hour, or day level.

Limits

Limits on API Gateway products and business.

Restrictions	Description
User restrictions on activating the API Gateway service.	To activate the service, you must complete the real-name registration.
Restrictions on the number of API groups created by a user.	Each account can have at most 100 API groups.
Restrictions on the number of APIs created by a user.	At most 1000 APIs can be created in each API group. That is, at most 100,000 (100 * 1000) APIs can be created in each account.
Restrictions on the number of independent domain names bound to an API group.	At most five independent domain names can be bound to a group.
The limit of the official subdomain.	When the API group is created successfully, the API gateway issues a secondary domain name for that group. You can test the API in the group by accessing the domain name, and the gateway restricts the number of visits to 1000 times per day. Please do not use the secondary domain name to provide API service directly.
Restrictions on parameter size.	The parameters of the body location (including Form and Form other forms) cannot exceed 2 Mb, and other locations (including Header and Query) cannot exceed 128 Kb.