API Gateway

HTTP Error Codes

Product Documentation

HTTP Error Codes

Last updated：2023-12-22 10:10:46

What are the common errors when API Gateway is called?

When you call API Gateway, you may encounter the following common HTTP error codes:

Frontend errors:

Error Code	Log Message	Description
401	HMAC apikey is invalid for API.	`APIKey` is not bound to this API.
401	HMAC signature cannot be verified, a valid x-date header is required for HMAC Authentication.	HMAC authentication does not include `x-date` in the header, or the HMAC value is invalid.
401	HMAC signature cannot be verified, the x-date header is out of date for HMAC Authentication.	The `x-date` timestamp timed out. It is 900s by default.
401	HMAC signature cannot be verified, a valid date or x-date header is required.	If there is no `x-date`, the header must contain `date`.
401	HMAC id or signature missing.	The ID or signature field is missing in `Authorization`.
401	HMAC do not support multiple HTTP header.	A header with multiple values is not supported.
401	HMAC signature cannot be verified, a valid xxx header is required.	xxx header is missing in the request.
401	HMAC algorithm xxx not supported.	HMAC algorithm does not support xxx, which currently supports HMAC-SHA1, HMAC-SHA256, HMAC-SHA384, and HMAC-SHA512.
401	HMAC authorization format error.	Incorrect `Authorization` format.
401	HMAC authorization headers is invalidate.	`Authorization` lacks sufficient parameters. For more information, please see Key Pair Authentication - Eventually Delivered Content.
401	HMAC signature cannot be verified.	Unable to verify the signature, possibly because the `APIKey` cannot be recognized. This usually

		happens if the `APIKey` is not bound to this service or API.
401	HMAC signature does not match.	The signature does not match.
401	Oauth call authentication server fail.	Failed to call the authentication server.
401	Oauth found no related Oauth api.	As the associated Oauth authentication API is not found, the `id_token` cannot be verified.
401	Oauth miss Oauth id_token.	The `id_token` is missing in the request.
401	Oauth signature cannot be verified, a validate authorization header is required.	Authentication header missing.
401	Oauth authorization header format error.	Incorrect Oauth header format.
401	Oauth found no authorization header.	Authentication header not found.
401	Oauth found no id_token.	`id_token` not found.
401	Oauth id_token verify error.	JWT-formatted `id_token` verification failed.
403	Found no validate usage plan.	No corresponding usage plan found. Access denied. (This error may occur if the usage plan feature is enabled.)
403	Cannot identify the client IP address, unix domain sockets are not supported.	Unable to identify the source IP.
403	Endpoint IP address is not allowed.	The backend IP is not allowed to access.
403	Get xxx params fail.	An error occurred while getting parameters from the request.
403	need header Sec-WebSocket-Key.	The `Sec-WebSocket-Key` header is missing in the actual request, which will be checked for APIs configured with WebSocket.
403	need header Sec-WebSocket-Version.	The `Sec-WebSocket-Version` header is missing in the actual request, which will be checked for APIs configured with WebSocket.
403	header xxx is required.	The xxx header is missing in the actual request.

403	path variable xxx is required.	The `{xxx}` path variable is configured but does not match the actual request path.
403	querystring xxx is required.	The xxx querystring is missing in the actual request.
403	req content type need application/x-www-form-urlencoded.	Requests with the `body` parameter must be in form format.
403	body param xxx is required.	The xxx body parameter is missing in the actual request.
404	Not found micro service with key.	No corresponding microservice found.
404	Not Found Host.	The request should have the `host` field, whose value should be the server's domain name in string type.
404	Get Host Fail.	The value of the `host` field in the request is not in string type.
404	Could not support method.	This request method type is not supported.
404	There is no api match host[$host].	Request server domain name/address not found.
404	There is no api match env_mapping[$env_mapping].	The `env_mapping` field after the custom domain name is incorrect.
404	There is no api match default env_mapping[$env_mapping].	The value of the `env_mapping` field after the default domain name should be `test/prepub/release` .
404	There is no api match uri[$uri].	The API that matches the URI is not found in the service corresponding to the request address.
404	Not allow use HTTPS protocol or Not allow use HTTP protocol.	The service corresponding to the requested address does not support the HTTP protocol type.
404	Found no api.	The request did not match an API.
405	Method Not Allowed.	HTTP request method not allowed
426	Not allow use HTTPS protocol.	HTTPS protocol not allowed.
426	Not allow use HTTPS protocol.	HTTP protocol not allowed.
426	Not allow use HTTPS protocol.	xxx protocol not allowed.
429	API rate limit exceeded.	The request rate limit is exceeded. The current rate can

		be viewed through the request header.
429	API quota exceeded.	The configuration quota is exceeded. Remaining quota can be viewed through the request header.
429	req is cross origin, api $uri need open cors flag on qcloud apigateway.	This is a cross-origin request, but the corresponding API has not enabled cross-origin access.
481	API config error.	API configuration error.
481	TSF config error.	TSF configuration error.
481	Get location of micro service info fail.	Microservice name and namespace are not configured to get location.
481	Only support the map_from like method.req.{path}.{}.	Microservice name and namespace are configured to get location, but the location format is invalid.
481	Found no valid cors config.	CORS configuration error.
481	Oauth public key error.	Public key certificate configuration error.
481	Oauth id_token location forbidden.	Forbidden `id_token` storage location.
481	Oauth found no oauth config.	Oauth configuration not found.
481	Oauth found no public key.	Public key not found.
481	Mock config error.	Mock configuration error.
499	Client closed connetion.	The client closed connection.

Backend errors:

Error Code	Log Message	Description
500	Error occurred during query params.	An error occurred while querying parameters.
500	Internal Server Error.	1. Other APIGW internal logic error. 2. If the API is proxy type, accessing the backend address without access permission will also cause this error.
502	Bad Gateway.	Backend service connection error. Possible reasons: 1. The backend denied the service, and the 502 error occurred for all requests.

		2. 2.Backend load was too high, and the 502 error occurred for some requests.
504	Gateway Time-out.	Backend server connection timed out.