API Gateway

FAQs

FAQs

If the API request reaches the gateway, the gateway returns the request result message.

You need to check the request header in the returned result. Results starting with X-Ca are all returned from the gateway. The important message contained in the result includes:

```
X-Ca-Request-Id: 7AD052CB-EE8B-4DFD-BBAF-EFB340E0A5AF
//The unique ID of the request. Once the request reaches the API gateway, the API gateway generates a request ID
and returns it to the client through the response header. We recommend that you record the request ID in both the
client and backend services for troubleshooting and tracing.

X-Ca-Error-Message: Invalid Url
//An error message returned from the API Gateway. When a request fails, the API Gateway returns the error
message to the client through the response header.

X-Ca-Debug-Info: {"ServiceLatency":0,"TotalLatency":2}
//A debug message returned when the debug mode is enabled. The message can be changed later and is used only
for reference at the debugging stage.
```

The header in X-Ca-Error-Message essentially clarifies the error cause. The X-Ca-Request-Id can be provided to technical support engineers for log searching.

The returned result of an HTTP/HTTPS request consists of the HTTPCode, Header, and Body. When a request fails, the returned Body may be empty because the request does not enter the business logic. The error “The return value is empty.” is returned. However, the important portion of the message is contained in the Header.

If an API request initiated by a user reaches the gateway, the gateway returns the result message indicating a request success or failure.

The majority of the returned messages are contained in the Header. Messages starting with X-Ca are returned from the gateway. Important messages include:

```
X-Ca-Request-Id: 7AD052CB-EE8B-4DFD-BBAF-EFB340E0A5AF
//The unique ID of the request. Once the request reaches the API gateway, the API gateway generates a request ID
and returns it to the client through the response header. We recommend that you record the request ID in both the
client and backend services for troubleshooting and tracing.

X-Ca-Error-Message: Invalid Url
//An error message returned from the API Gateway. When a request fails, the API Gateway returns the error
message to the client through the response header.

X-Ca-Debug-Info: {"ServiceLatency":0,"TotalLatency":2}
```

```
//A debug message returned when the debug mode is enabled. The message can be changed later and is used only for reference at the debugging stage.
```

Therefore, if the returned message of a request is empty, check the returned Header. In normal cases, the Body is empty when the request reaches the gateway and an error is returned stating "The return value is empty." However, the important portion of the message is contained in the Header.

If the Header is also empty, the request did not reach the gateway. You need to check your network conditions.

You can search for methods to obtain and view the HTTP/HTTPS request headers in different languages.

Error message

The certificate authentication error or certificate expiration prompt is returned during an HTTPS interface call.

Cause and solution

1. Invalid certificate

The certificate of the API provider is issued by a non-mainstream organization, however, it can be used for browser access because the browser automatically updates the root certificate. However, the root certificate for an operating system of an earlier version does not trust the certificate issuance organizations, or the trust has expired.

Solution

1. Update the client root certificate. For example, for Java+Linux, update the OpenSSL client. For other operating systems and programming languages, update the root certificate used by HTTPS in the programming language.
2. Contact the API provider to change to a mainstream SSL certificate with better compatibility.
3. The SSL certificate validity check is omitted in the program. However, this configuration is not recommended because the request may be hijacked. The method should only be used when the API provider cannot provide a mainstream SSL certificate with better compatibility and the security risk is controllable.

2. Invalid SSL certificate of the API provider

The SSL certificate of the API provider expires.

Solution

1. Contact the API provider to change the SSL certificate.
2. The SSL certificate validity check is omitted in the program. However, this configuration is not recommended because the request may be hijacked. The method should only be used when the API provider cannot provide a mainstream SSL certificate with better compatibility and the security risk is controllable.

Public error codes

Scenarios	Error code		Status code	Suggestion
The domain is invalid (the product cannot be found based on the domain).	InvalidProduct.NotFound		404	Check whether the called domain or the domain in product configurations is correct.
API is missing. The API is the Private type, and the user is not in the list.	InvalidApi.NotFound		404	Check whether the called API is correct. Pay attention to case sensitiveness, and check whether access control is enabled.
API must be based on HTTPS.	InvalidProtocol.NeedSsl		400	Check whether API only supports HTTPS.
The required parameter is missing (enter the actual parameter name in {}).	Missing{ParameterName}		400	Check whether you have entered the parameter during the call process.
AccessKeyID is missing.	InvalidAccessKeyId.NotFound		404	Check whether a correct AccessKeyID is used for the call.
AccessKeyID is disabled.	InvalidAccessKeyId.Inactive		400	Check whether the AK is valid, or whether the AK matches the environment.
The time stamp is	InvalidTimeStamp.F		400	Check the time

invalid (Date and Timestamp).	ormat			stamp.
The difference between the user time and server time exceeds 15 minutes.	InvalidTimeStamp.Expired		400	Check the time stamp.
SignatureNonce is repeated.	SignatureNonceUsed		400	
MD5 verification fails (ROA).	ContentMD5NotMatched		400	
The format of the returned value is invalid (the format is not supported).	InvalidParameter.Format		400	The XML or JSON format is supported. ROA supports application/json and application/xml.
The format of the returned value is invalid (Accept is not supported).	InvalidParameter.Accept		400	
Parameter value validation fails.	Invalid{ParameterName}		400	
The HTTP request method is not supported (request method allowed in previous API configurations).	UnsupportedHTTPMethod		400	
The signature method is not supported.	InvalidSignatureMethod		400	
The server-side position is incorrect.	InternalError		500	
The service is unavailable temporarily (the underlying service is unavailable).	ServiceUnavailable		503	View the ISP protocol description in API configurations, and check whether the service provided by the connected party is normal.

Invalid signature	SignatureDoesNotMatch		400	For details about invalid signature, refer to Signature Verification.
Parameter values do not match (the parameters in URL and body do not match).	ValueMismatch.{ParameterName}		400	
The user’s traffic within the current period of time has exceeded the upper limit.	Throttling.User			
The API traffic within the current period of time has exceeded the upper limit.	Throttling.Api			
The specified content-length does not match the body length.	ContentLengthDoesNotMatch		400	
The specified parameter is repeated.	RepeatedParameter. {ParameterName}		400	
The user’s traffic within the current period of time has exceeded the upper limit.	Throttling.User		400	
The API traffic within the current period of time has exceeded the upper limit.	Throttling.Api		400	
AccessKeyId is missing.	MissingSecurityToken		400	Token authentication logic is applied when AccessKeyId starts with “STS.”. The error is returned when AccessKeyId starts with “STS.” but the SecurityToken parameters,

				including RPC and ROA, are not input.
SecurityToken expires.	InvalidSecurityToken.Expired		400	Check the SecurityToken.

Client errors (activating an API)

Error code	Description	HTTP status code	Meaning	Solution
Repeated%s	The specified %s is repeated.	400	A parameter is repeated. %s is a placeholder and a specific parameter name or prompts are provided when you call an API.)	Follow the prompts to modify the repeated parameter and try again.
RepeatedCommit	Resubmit request.	400	The request is repeated.	Do not submit the request frequently.
Missing%s	The %s is mandatory for this action.	400	The parameter %s is missing.	Enter the missing parameter according to the error and try the request again.
MissingAppIdOrAppOwner	AppId or AppOwner must have a valid value.	400	AppId or AppOwner is missing.	AppId and AppOwner cannot both be empty.
Invalid%s	The specified parameter %s value is not valid.	400	The parameter is invalid.	Follow the prompts to enter the specific parameter, view restrictions on parameters, and try again.
NotFound%s	Cannot find resource according to your specified %s.	400	The resource is not found.	The resource cannot be found based on the specified parameter %s. Check whether %s is correct.

InvalidFormat%s	The specified parameter %s value is not well formatted.	400	Parameter format is incorrect.	Follow the prompts to check and modify the format of %s and try again.
Duplicate%s	The specified parameter %s value is duplicate.	400	The parameter is repeated.	Duplicate request parameters are not allowed. Check and modify the parameter and try again.
DependencyViolation%s	The specified %s has %s definitions.	400	The parameter dependency is incorrect.	The specified parameter that others are dependent on cannot be deleted. Remove the dependency and then delete the parameter.
Forbidden%s	Not allowed to operate on the specified %s.	403	Operation is not permitted/the operation is prohibited.	You are not permitted to perform the operation.
NoPermission	User is not authorized to operate on the specified resource.	403	Operation is not permitted.	RAM authentication fails.
ExceedLimit%s	The specified %s count exceeds the limit.	400	The quota is exceeded.	The number of APIs, API groups or APPs created in the user account exceeds the quota.
UserNotFound	The specified user can not be found.	404	The specified user cannot be found.	The user cannot be found based on the input user information.
DomainCertificateNotFound	Cannot find the domain certificate.	400	The specified domain name certificate does not exist.	Check the ID and name of the input certificate.
DomainNotResolved	The specified domain has not	400	The specified domain name	You need to resolve the

	been resolved.		is not resolved.	CNAME of the specified domain name to a second-level domain name of the group and then bind the specified domain name to the second-level domain name. The domain name should be resolved on the website from which you buy the domain name.
InvalidICPLicense	The specified domain have not got ICP license, or the ICP license does not belong to Aliyun.	400	The domain name filing fails.	The domain name to be bound should be firstly filed with Alibaba Cloud. Domain names filed with other systems should be filed for access to Alibaba Cloud. A filing number is needed for access filing. Each of ECS instances filed with Alibaba Cloud and having public IP addresses have five filing numbers.
Invalid%s.LengthLimit	The parameter %s length exceeds the limit.	400	The parameter is too long.	The parameter %s is too long. Modify the parameter and try again.
InvalidApiDefault	The ApiDefault value exceeds limit.	400	The default API traffic control value exceeds the quota.	The value cannot exceed 1,000,000,000, regardless of the unit. For a higher quota, you need to submit a ticket.

InvalidAppDefault	The AppDefault value must smaller than the UserDefault and ApiDefault.	400	The AppDefault value does not comply with the rules.	The value must be less than the API traffic control value and the user traffic control value.
InvalidUserDefault	The UserDefault value must bigger than the AppDefault and smaller than the ApiDefault.	400	The UserDefault value does not comply with the rules.	The value should be less than the API traffic control value but greater than the APP traffic control value.
InvalidParamMapping	Parameters must be fully mapped.	400	Parameter mapping is invalid.	API creation requires full mapping between front-end and backend parameters. That is, a backend parameter name needs to be configured for each input parameter.
InvalidOwnerAccount	OwnerAccount is invalid.	400	The APP owner account is invalid.	The Alibaba Cloud Mail account of the target user entered during operation authorization is invalid. Check and modify the account and try again.
ServiceForbidden	Your Gateway service is forbidden by risk control.	400	The API Gateway service is forbidden by risk control policies (the user should be forbidden by risk control policies).	Do not submit the request frequently. Try again later. If the problem persists after retry, submit a ticket for consultation.
ServiceUnOpen	Your Gateway service has not been opened.	400	The service is not activated.	Activate the API Gateway service at Alibaba Cloud website.

ServiceInDept	Your API Gateway service is in dept.	400	(Your API Gateway) service is in arrears.	The service can be used after account recharge or bill settlement.
EqualSignature	The new signature is the same as the old.	400	The new signature key is the same as the old one.	The modified backend signature key and secret cannot be the same as the old ones.
CertificateNotMatch	The domain does not match the one in the certificate.	400	The domain name does not match that in the certificate.	The specified domain name does not match that in the certificate.
CertificateKeyNotMatch	The certificate private key does not match the public key.	400	The certificate keys do not match each other.	The certificate public key does not match with the private key.
PrivateKeyEncrypted	The certificate private key is encrypted, please upload the unencrypted version.	400	The private key cannot be encrypted.	The certificate private key is encrypted, but the unencrypted version should be uploaded.
CertificateSecretKeyError	The certificate private key is invalid.	400	The certificate private key is invalid.	Check and upload the private key again.
InvalidApiServiceAddress	The specified service address is not valid.	400	The API backend service address is invalid.	The configured API backend service address is invalid.

Client errors (calling an API)

Error code	HTTP status code	Meaning	Solution
Throttled by USER Flow Control	403	The operation is throttled by user flow control policies.	Generally, the operation is throttled by the flow control policies due to the user flow control value set by the API service provider. You can contact the API service provider for a higher user flow

			control value.
Throttled by APP Flow Control	403	The operation is throttled by APP flow control policies.	Generally, the operation is throttled by flow control policies due to the APP flow control value set by the API service provider. You can contact the API service provider for a higher APP flow control value.
Throttled by API Flow Control	403	The operation is throttled by API flow control policies.	Generally, the operation is throttled by flow control policies due to the API flow control value set by the API service provider. You can contact the API service provider for a higher API flow control value.
Throttled by DOMAIN Flow Control	403	The operation is throttled by flow control on the second-level domain name.	The second-level domain name used for API calls can be accessed up to 1,000 times each day.
TThrottled by GROUP Flow Control	403	The operation is throttled by group flow control policies.	Each group has limited QPSs. Feed back the problem to the API service provider.
Quota Exhausted	403	The call quota is exhausted.	The call quota you have bought is exhausted.
Quota Expired	403	The quota you have bought expires.	The quota you have bought expires.
User Arrears	403	The account is in arrears.	Recharge your account as soon as possible.
Empty Request Body	400	The body is empty.	Check the content of the request body.
Invalid Request Body	400	The body is invalid.	Check the request body.
Invalid Param Location	400	The parameter location is incorrect.	The location of the request parameter is incorrect.

Unsupported Multipart	400	Upload is not supported.	The file upload is not supported.
Invalid Url	400	URL is invalid.	The requested method, path or environment is incorrect. For details, refer to [Invalid URLfor error description.
Invalid Domain	400	The domain name is invalid.	The request’ s domain name is invalid and API cannot be found based on the domain name. Contact the API service provider.
Invalid HttpMethod	400	The HTTPMethod is invalid.	The HTTPMethod is entered incorrectly.
Invalid AppKey	400	AppKey is invalid or does not exist.	Check the input AppKey and keep no spaces at either side of the parameter.
Invalid AppSecret	400	AppSecret is incorrect.	Check the input AppSecret. keep no spaces at either side of the parameter.
Timestamp Expired	400	The timestamp expires.	Check whether the request system time is a standard time.
Invalid Timestamp	400	The timestamp is invalid.	For details, refer to Request signature description.
Empty Signature	404	The signature is empty.	Refer to Request signature description for how to input the signature string.
Invalid Signature, Server StringToSign:%s	400	The signature is invalid.	Refer to Invalid signature for signature invalidity errors.
Invalid Content-MD5	400	The Content-MD5 value is invalid.	The request body is empty but the MD5 value is entered or the MD5 value calculation is incorrect. For details, refer to Request signature description.

Unauthorized	403	The operation is unauthorized.	The APP is unauthorized for API calls. Refer to Unauthorized for error instructions.
Nonce Used	400	The SignatureNonce is used.	The SignatureNonce cannot be used repeatedly. For details, refer to Signature Mechanism.
API Not Found	400	The API cannot be found.	The input GroupId, Stage or other parameters are incorrect or the API is deprecated.

Server errors (opening an API)

Error code	Description	HTTP status code	Meaning	Solution
ServiceUnavailable	The request has failed due to a temporary failure of the server.	503	Service is unavailable.	Try again.
InternalError	The request processing has failed due to some unknown error, exception or failure.	500	There is an internal error.	Try again.

Server errors (calling an API)

Error code	HTTP status code	Meaning	Solution
Internal Error	500	The API Gateway has an internal error.	Try again.
Failed To Invoke Backend Service	500	The underlying service has an error.	An error occurred in the underlying API service. Try again and contact the API service provider for a solution if the problem persists after several retries.
Service Unavailable	503	Service is unavailable.	Try again later.

Cause of error

You may get an error when the request HTTP Schema is incorrect. Different APIs support different HTTP Schemas. API providers can set the APIs to support either or both HTTP and HTTPS requests.

The prompt “API unsupport the channel: HTTP” is returned when the API only supports HTTPS, but HTTP is used during API request.

The prompt “API unsupport the channel: HTTPS” is returned when the API only supports HTTP, but HTTPS is used during API request.

Solution

When the prompt “API unsupport the channel: HTTP” is returned, change HTTP to HTTPS and initiate the API call again.

When the prompt “API unsupport the channel: HTTPS” is returned, change HTTPS to HTTP and initiate the API call again.

Cause of error

The signature at the client does not match the signature at the server.

Solution

When the signatures do not match, the gateway returns the StringToSign of the server signature through an X-Ca-Error-Message in the HTTP Response Header.

StringToSign is a string added before your request and used for signature computing. For details, refer to Request Signature Instructions.

StringToSign added locally at the client needs to be printed and checked for any differences. If the call demo provided by Alibaba Cloud is used, you can find the StringToSign before signature computing in the signature computing tools. Print this and check for any discrepancies.

Linefeed is not allowed in the HTTP Response Header, and linefeeds in StringToSign in the returned results are omitted. Compare the returned StringToSign with that in the reference documentation.

If StringToSigns at the server and client are consistent, check whether the AppKey and AppSecret used are correct. Particularly, check whether any spaces or other characters, that are not easily identifiable, have been added.

Cause of error

The HTTP Method, Path, or specified stage (X-Ca-Stage) of the request is incorrect.

For example, an API is specified to be called in the test stage, but the API is not released to the test stage.

Note:

- If a stage isn’ t specified for the request, APIs in the release stage are accessed by default.
- An API where the definition is modified should be released again to take effect. In most cases, the path is modified, but the API has not been released again. An error is reported when the request is submitted based on the new path.

Solution

Check the three factors: HTTP Method, Path, and stage.

1. If POST request is required in API instructions, GET requests are not supported. The call methods should be consistent.
2. The request path should be consistent with the current running path. APIs that are modified, but not released, can result in a call failure.
3. An appropriate stage should be specified. The value of the parameter X-Ca-Stage in the request Header is “RELEASE/TEST”, indicating the test and online stages, respectively. If this parameter is left empty, the online stage is used by default.
4. For more instructions on parameters and requests, refer to Call an API.

Cause of error

When requesting an API, the app that the AppKey belongs to is unauthorized to call the API.

Solution

Factors determining authorization validity include app, API, stage, and authorization.

1. If you are an open API user and use the app for testing, you need to create an app on the API Gateway Console. Then use the AppId to authorize the app on the API list page. For a self-testing purpose, the open API user needs to authorize the created app.
2. If you bought an API, you can check the authorized APIs of this app on the app details page. If the API to be called is not authorized, authorize the desired API.
3. If you use a partner’ s API instead of buying one, contact your partner and provide your AppId for authorization by the API provider.
4. The authorization is subject to the stage. When the app and API are in the same stage, the authorization and request should also be in the same stage. When an API is authorized in the A stage, services of the API in the B stage cannot be called. For details about the

request stage and other parameters, refer to API request sample.

5. The most important thing is to check whether the wrong app is used or whether an incorrect API is called. There are many APIs and apps, and sometimes they get mixed up and result in a call failure. For example, the app in the A stage is authorized, but the app in the B stage is called. Ensure all care is taken when calling the apps.

You need to check whether the entered backend service address is correct and ensure that the backend service can be accessed normally. If your backend service is on ECS, check the security group settings to see if it can be accessed externally. Ensure that the security group allows access to the IP section of the API gateway.

```

- North China 1 (Qingdao): 10.151.203.0/24

- North China 2 (Beijing): Internet: 123.56.213.0/24, Intranet: 10.152.167.0/24

- Southern China 1 (Shenzhen): Internet: 120.76.91.0/24, Intranet: 10.152.27.0/24

- East China 1 (Hangzhou): Internet: 114.55.70.0/24, Intranet: 10.152.29.0/24, 10.152.30.0/24

- East China 2 (Shanghai):
```

10.152.163.0/24,10.152.164.0/24,11.192.97.0/24,11.192.98.0/24,11.192.96.0/24

```

- Hongkong:
```

10.152.161.0/24,10.152.162.0/24

```

- Southeast Asia 1 (Singapore):
```

10.152.165.0/24,10.152.166.0/24,11.192.152.0/23,11.193.8.0/24,11.193.9.0/24

- If you are using an intranet IP, make sure your backend services are in the same Region as your APIs.