Response Codes and Errors

Description

Following is the full list of Gigya response codes and error codes.

0 indicates success while 20000**x** codes indicate a response; all other codes indicate an error.

A validation error is returned whenever there is a data validation error regarding one of the following required fields:

- username
- password
- secretQuestion
- secretAnswer
- email

Error Code Definitions Table

errorCode	errorMessage	Description
0		Success.
100001	Data pending	Data is still being processed. Please query again for the response.
200001	Operation canceled	User canceled during the login process.
200008	OK with errors	For reports purposes, when OK is returned but there were acceptable errors in the process.
200009	Accounts linked	The accounts have been linked successfully.
200010	OK with error login identifier exists	When a new account is created and the login identifier already exists, the server handles the conflict according to the **conflictHandling** parameter. If **saveProfileAndFail** is passed, the profile data is saved, a registration token is returned for account linking, and this error is returned.
206001	Account pending registration	A method has been called that performs social login, but the registration process has not been finalized, or a required field is missing from the user profile or data. See Accounts API Error Codes and Messages for more information.
206002	Account pending verification	An account has already been verified and a user tries to log in with a loginID (usually an email address) whose connection to the user has not been verified. See Accounts API Error Codes and Messages for more information.
206003	Account missing loginID	The registration policy requires a loginID when a user uses Social Login to register to the site, but there are no login identifiers or a password associated with the account. See Accounts API Error Codes and Messages for more information.
206004	Identities were conflicted	An identity conflict has occurred during account import. This means that a providerUID being imported matches one that is already in the system.
206005	Pending Autologin Finalization	When auto-login from email verification link policy is activated, this response code is passed as the user is redirected to the nextURL specified in the policy. It is not indicative of an error.
301001	Invalid data center	The API key is served by another data center. The error occurs when an API request is received at the wrong data center.
400001	Invalid request format	This error may be caused by various faults in the request. For example: - wrong authentication header - non-secure request that should be secured.

400002	Missing required parameter	The method requires some parameters. One of the required parameters was not set in this method call. The error message will include the name of the missing parameter.
400003	Unique identifier exists	A user tries to register or set the account information with an email or username that already exists in the accounts database. See Accounts API Error Codes and Messages for more information. Some possible response messages are: • If a chosen Username already exists the returned message is **Username already exists**. • If a chosen Email already exists the returned message is **Email already exists**.
400004	Invalid parameter format	One of the parameters of this request has been set with a value which is not in the expected format.
400006	Invalid parameter value	One of the parameters of this request has been set with a value which is not within the parameter's defined value bounds. Please refer to the method's parameter table, and check the definition of valid values per parameter. The error message will include the name of the specific parameter.
400007	Duplicate value	Internal error.
400008	Invalid authentication header	An OAuth2 error. See OAuth2 Error Response for more information.
400009	Validation	In accounts.register, whenever there is a validation error. Some possible response messages are: • If input Password Doesn't meet policy requirements (or is larger than 30 characters) the returned message is "Password does not meet complexity requirements". • If input Password Confirmation does not match Password field the returned message is **Passwords do not match**. • If any Invalid or unsupported input (all fields) is detected the returned message is **Invalid %fieldname**.
400011	Invalid redirect URI	An OAuth2 error. See OAuth2 Error Response for more information.
400012	Invalid response type	An OAuth2 error. See OAuth2 Error Response for more information.
400013	Unsupported grant type	An OAuth2 error. See OAuth2 Error Response for more information.
400014	Invalid grant	An OAuth2 error. See OAuth2 Error Response for more information.
400015	Code expired	An OAuth2 error. See OAuth2 Error Response for more information.
400020	Schema validation failed	There was an attempt to write to fields from the client side. By default, only signed requests coming from the server are allowed to write into the data fields.
400021	CAPTCHA verification failed	The registration policy requires the user to pass a CAPTCHA test in order to register and the CAPTCHA verification has failed. See Accounts API Error Codes and Messages for more information.
400022	Unique index validation	Used mostly for DS, where custom unique indexes are supported.
400023	Invalid type validation	When the internal type (string, int, date, etc) does not match the type of the provided value.
400024	Dynamic fields validation	A validation error is returned whenever there is a data validation error regarding one of the following required fields: username, password, secretQuestion, secretAnswer, email.
400025	Write access validation	A write access error regarding one of the following required fields: • **username** • **password** • **secretQuestion** • **secretAnswer** • **email**
400026	Invalid format validation	Invalid regex format.

400027	Required value validation	A required value is missing or has an error in one of the following required fields:
		username **password** **secretQuestion** **secretAnswer** **email** Some possible response messages are: - If CAPTCHA input is blank or incorrect the returned message is "The characters you entered didn't match the word verification. Please try again". - If a required field (all fields) is not complete the returned message is "This field is required".
400028	Email not verified	The email address provided has not been verified.
400029	Schema conflict	An internal error was encountered while indexing the object.
400030	Operation not allowed	This error is returned if a user logs in with a SAML provider, and multiple identities are not allowed, and a call to socialize.addConnection or to socialize.removeConnection is attempted.
400031	Regex too complex	This error is returned if your implementation includes a custom regex for validating the email format of the **profile.email** field in registration screens (defined using accounts.setSchema), and the regex is so complex that it impedes performance.
400050	Security verification failed	With accounts.resetPassword when the provided credentials could not be verified.
400093	Invalid ApiKey parameter	The provided API key is invalid.
400096	Not supported	The function is not supported by any of the currently connected providers.
400097	Browser insecure	The user is attempting to access Gigya services from an insecure/unsupported browser. User should switch browsers.
400100	No providers	With accounts.tfa.importTFA or accounts.tfa.resetTFA when no such TFA provider exists.
400103	Invalid containerID	The containerID specified does not exist.
400106	Not connected	User is not connected to the required network or to any network.
400120	Invalid site domain	The current domain does not match the domain configured for the api key. This error may also be returned if the URL is behind a firewall or is otherwise not publicly available. When sharing or shortening URLs via any Gigya Add-ons, APIs, or methods, the URL being used must be a publicly accessible URI. If the URI is behind a firewall, an HTTP Auth, or does not respond within 5 seconds of a request to retrieve the URL of the page, even if the URL is within a whitelisted domain, Gigya will respond with errorCode **400120** - **Invalid Site Domain**, and the request will fail.
400122	Provider configuration error	An error originated from a provider.
400124	Limit reached	Refers generally to any reached limits, either in Loyalty or in Comments. In Loyalty, when a user performed more actions than the allowed daily cap (maximum actions per 24 hrs), or when a user performed actions more frequently than the allowed frequency cap (minimum interval between consecutive actions). So the error can be **DailyCap exceeded** or **FreqCap exceeded**. In commenting, the error is returned when a user reaches the daily limit of new comments threads per stream.
400125	Frequency limit reached	A comments spam cap was reached.
400126	Invalid action	In Gamification when the action is invalid.
400127	Insufficient points to redeem	When the gamification method **redeemPoints** is called, and the user does not have enough points, the operation fails and this error occurs.
401000	Invalid policy configuration	If Protect Against Account Harvesting policy is enabled and neither Email Validation nor CAPTCHA Validation policies are enabled.

401001	Media items not supported	When media items are not allowed for this category.
401010	Suspected spam	If someone is trying to use Gigya to send an email with a URL that does not match any of the client's domains.
401020	Login Failed Captcha Required	If accounts.login is attempted and the CAPTCHA threshold has been reached. The CAPTCHA threshold is set in the site Policies (**security.captcha.failedLoginThreshold** policy).
401021	Login Failed Wrong Captcha	If accounts.login is attempted and the CAPTCHA threshold has been reached and the provided CAPTCHA text is wrong. The CAPTCHA threshold is set in the site Policies (**security.captcha.failedLoginThreshold** policy).
401030	Old password used	The password provided is not the correct *current* password, however, it is a password previously associated with the account. This may appear in the following cases: • When accounts.login is attempted with a password that doesn't match the current password but does match the previous one, the server will return this error with a message saying that "the password was modified on" the date when the current password was set. • When accounts.resetPassword is attempted with a password that has previously been used with the account, the server will return this error with a message stating "invalid password: the provided password was already in use by this account".
403000	Forbidden	You do not have permission to invoke the method.
403002	Request has expired	The timestamp or expiration of the token used exceeded the allowed time window. The most common cause for this error is when your server's clock is not accurately set. This causes a gap between your time and Gigya's time. Even a gap of two minutes is enough to create this error. Please refer to Signing requests for more details.
403003	Invalid request signature	The request is not signed with a valid signature. Please refer to Signing requests for more details.
403004	Duplicate nonce	The value of the nonce parameter that was passed with this request is not unique. Gigya requires that in each REST API call the nonce string will be unique. If Gigya receives two API calls with the same nonce, the second API call is rejected. Please refer to Signing requests for more details.
403005	Unauthorized user	The user ID that is passed is not valid for this site.
403006	Secret Sent Over Http	When sending the secret key in REST it has to be over HTTPS.
403007	Permission denied	Returned when a user lacks the necessary permissions to perform the requested action, or when the user's credentials are not configured properly.
403008	Invalid OpenID Url	Cannot find an openId endpoint on the url or cannot find the username given for the openId login.
403009	Provider session expired	The user session for this provider has expired.
403010	Invalid Secret	The request has an invalid secret key.
403011	Session has expired	The session for this user has expired.
403012	No valid session	Requested user has no valid session.
403013	Unverified User	The user is not registered on the site. Encountering this error within a Site Group situation means that accounts.verifyLogin was not called on the destination site.
403015	Missing request referrer	We can't validate the request because the referrer header is missing.
403017	Unexpected provider user	The user currently logged in to the requested provider is not the same as the one logged in to the site.
403022	Permission not requested	This operation needs a user permission and it was not requested. You may use the method socialize.requestPermissions to request the user permission. After gaining user permission you may retry to execute this operation.
403023	No user permission	This operation needs a user permission and the user did not grant your application with the necessary permission.

403024	Provider limit reached	Limit reached: Status is a duplicate. This error occurs when a user shares content multiple times, and is returned with the provider name, e.g., "provider" : "twitter".
403025	Invalid token	Invalid OAuth2 token. Read more in Using Gigya's REST API in compliance with OAuth 2.0.
403026	Unauthorized access error	Returned from the accounts.isAvailableLoginID method, when Protect Against Account Harvesting policy is enabled.
403031	Approved by moderator	Can't flag comment, it was already approved by a moderator.
403035	No user cookie	The request is missing user credentials.
403036	Unauthorized partner	The relevant Gigya product is not enabled for this partner.
403037	Post denied	Comments - Post denied when the user tried to review twice.
403040	No login ticket	No login ticket in callback URL.
403041	Account disabled	A user has tried to log into an inactive account. See Accounts API Error Codes and Messages for more information.
403042	Invalid loginID	A user passes an incorrect password or a login ID that doesn't exist in our accounts database. See Accounts API Error Codes and Messages for more information.
403043	Login identifier exists	The username/email address provided by the user exists in the database but is associated with a different user. See Accounts API Error Codes and Messages for more information.
403044	Underage user	A user under the age of 13 has tried to log in. For COPPA compliance (Children's Online Privacy Protection Act). Please refer to the Age Limit section in the Policies guide.
403045	Invalid site configuration error	If Customer Identity (RaaS) is enabled for your site, but the storage (DS) size has not been configured.
403047	Login ID does not exist	There is no user with that username or email. In the "Forgot Password" screen of a Gigya Screen-Set, this error is returned if a user fills in an email of a user that doesn't exist.
403048	API Rate Limit Exceeded	The daily API call limit has been reached.
403051	Ip Blocked	The IP address attempting to connect to Gigya does not have permission.
403100	Pending password change	When accounts.login is attempted and the password change interval has passed since the last password change. The interval is set in the site Policies (**security.passwordChangeInterval** policy).
403101	Account Pending TFA Verification	When accounts.login, accounts.socialLogin, accounts.finalizeRegistration, socialize.notifyLogin, or socialize.login is called and the RBA policy requires two-factor authentication, and the device is not already in the verified device list for the account. The first time the method is called, the device needs to be registered, and for the following calls, the device needs to be verified.
403102	Account Pending TFA Registration	When accounts.login, accounts.socialLogin, accounts.finalizeRegistration, socialize.notifyLogin, or socialize.login is called and the RBA policy requires two-factor authentication, and the device is not already in the verified device list for the account. The first time the method is called, the device needs to be registered, and for the following calls, the device needs to be verified.
403110	Account Pending Recent Login	When there is an attempt to deactivate a TFA provider for a user (with accounts.tfa.deactivateProvider) or to register a user (with accounts.tfa.initTFA) and the user did not log in through the device in the last few minutes.
403120	Account Temporarily Locked Out	When accounts.login is attempted and the account is locked out or the originating IP is locked out. This occurs after a set number of failed login attempts. This number is configured in the site's RBA Policies.
403200	Redundant operation	When the client performs an operation that is redundant.
403201	Invalid application ID	When the provided app ID is different from the one configured for the site.
404000	Not found	When returned from a **comments** API: **category not found**. When returned from an **accounts** API: **email verification failed**.

404001	Friend not found	The friend user ID provided is not a friend for the current user.
404002	Category not found	Comments - Category not found.
404003	UID not found	Caused by an invalid UID, or a UID not applicable to the current API key.
404004	Invalid URL	An embed.ly 404 error message returned when the URL is invalid.
405001	Invalid API method	Internal for Gigya JavaScript Web SDK.
409001	Identity exists	When attempting to connect to a provider that is already connected or to link to an already linked account.
409002	Social provider exists in account	When attempting to link an account to a social provider, but that social provider already exists in the account, under a different email.
409010	Missing user photo	When calling accounts.getProfilePhoto, accounts.publishProfilePhoto or accounts.uploadProfilePhoto. The user photo requested does not exist or the photo provided is not valid.
409011	Counter not registered	There was an attempt to set or retrieve information in a counter that the system cannot find. See accounts.incrementCounters.
409012	Invalid gmid ticket	See 3rd Party Cookies for information about using gmid tickets.
409013	SAML mapped attribute not found	When a mapped attribute value for the providerUID cannot be retrieved.
409014	SAML certificate not found	When the SAML certificate cannot be retrieved.
409030	Concurrent updates not allowed	When attempting to call an API for the same user/data with more than the maximum number of concurrent requests defined for that API.
409031	No provider session	When a request to a social provider is pending, but a required authToken is missing.
409040	CERT_INVALID_CNAME	A Cname failed to validate. Possible causes are apiPrefix is empty or the domain name was not found or there was a name mismatch.
410000	Gone	Resource is no longer available.
413001	Request entity too large	Comments plugin received a request that was too large.
413002	Comment text too large	Comments plugin received a comment with too much text.
413003	Object too large	The data store object size is too large, it is limited to 512KB.
413004	Profile photo too large	The profile photo exceeded file-size limits, or uses a non-supported format.
500000	General security warning	General security warning. When received while using any Gigya SDKs, this error means that the SDK could not connect to Gigya servers and does not mean there was an actual error received.
500001	General Server error	General server error.
500002	Server login error	General error during the login process.
500003	Default application configuration	For multiple Data Centers (DCs) when no default application can be found.
500014	Session migration error	Error while migrating old Facebook session to new Graph API Facebook session.
500023	Provider error	General error from the provider.
500026	Network error	Various network errors, e.g., when a JSONP request fails.
500028	Database error	General database error.
500031	No provider application	There is no definition of provider application for this site. Please refer to Opening External Applications to learn how to define a provider application.
500033	Invalid environment config	When there is no target environment in the config file.
500034	Error during backend operation	Internal error.
503001	Service unavailable for this operation	Too many calls were done with the same account UID within a specific time period.

504001	Timeout	Client-side error.
504002	Request Timeout	A timeout that was defined in the request is reached.
599999	Missing Error Code	This is the errorCode returned when there is no other specific errorCode defined for the error that occurred. You can find additional information in the **errorDetails** and/or **statusReason** fields (note that **statusReason** is a deprecated property and may not contain a value).

Unable to render {include}   The included page could not be found.

Additional Information

On certain occasions within Accounts APIs you may receive Validation Errors as sub errors of the primary error. This may occur whenever more than a single field is being validated as part of the originating API call. For more information, see Accounts API Validation Errors.