# API Signatures for GConnect

Contents

[API Signatures for GConnect 1](#_Toc18621719)

[Authentication APIs 3](#_Toc18621720)

[Register 3](#_Toc18621721)

[Get Access Token 4](#_Toc18621722)

[Get Refresh Token 5](#_Toc18621723)

## Authentication APIs

### Register

Client registration with client id (Its email) and secret (Its password). The secret is stored in database after encryption and is secure.

-- Password must include at least one upper case character (A-Z)

-- Password must include at least one lower case character (a-z)

-- Password must include at least one digit (0-9)

-- Password must include at least one special character (Punctuation)

-- Password should not start with a digit

-- Password should not end with a special character

**HTTP Method:** POST

**URL:** POST /ns/api/v1/auth/register

**Request Headers**

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Type | Required/Optional | Description |
| **clientId** | String | Required | Its unique id normally representing email |
| **secret** | String | Required | Represents password |

#### Response

**AuthResponseDTO {**

**accessToken** (string): represents the oAuth access token ,

**authorizeToken** (string, optional): represents the oAuth authorize token ,

**clientId** (string): represents the oAuth client id which is normally email ,

**code** (integer): http status codes like 200 for success ,

**error** (string): Have value if code is not 200, it provides the complete details about the error occured ,

**message** (string, optional): Message details in case of success or failure ,

**path** (string): URL for the invoked http resource ,

**refreshToken** (string): represents the oAuth refresh token ,

**timestamp** (Timestamp, optional): Represents current timestamp

**}**

**Timestamp {**

date (integer, optional),

day (integer, optional),

hours (integer, optional),

minutes (integer, optional),

month (integer, optional),

nanos (integer, optional),

seconds (integer, optional),

time (integer, optional),

timezoneOffset (integer, optional),

year (integer, optional)

**}**

**Sample response**

{

"code": 200,

"error": "",

"timestamp": "2019-07-11T11:34:05.116+0000",

"message": "",

"path": "/ns/api/v1/auth/register ",

"accessToken": "b6a29ed0f4174032bd991892021cc1ee",

"refreshToken": "cb53d097c5d742ce983dbf81a5011ee4",

"authorizeToken": “7c52c0aa8b6a48d09ede6aa4ff10e89f”,

"clientId": "test"

}

### Get Access Token

This API provides access token.

Access tokens are the thing that applications use to make API requests on behalf of a user. The access token represents the authorization of a specific application to access specific parts of a user’s data.

Access tokens must be kept confidential in transit and in storage. The only parties that should ever see the access token are the application itself, the authorization server, and resource server. The application should ensure the storage of the access token is not accessible to other applications on the same device. The access token can only be used over an https connection, since passing it over a non-encrypted channel would make it trivial for third parties to intercept.

The token endpoint is where apps make a request to get an access token for a user. This section describes how to verify token requests and how to return the appropriate response and errors.

**HTTP Method:** POST

**URL:** POST /ns/api/v1/auth/get/accesstoken

**Request Headers**

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Type | Required/Optional | Description |
| **clientId** | String | Required | Its unique id normally representing email |
| **secret** | String | Required | Represents password |

#### Response

**AuthResponseDTO {**

**accessToken** (string): represents the oAuth access token ,

**authorizeToken** (string, optional): represents the oAuth authorize token ,

**clientId** (string): represents the oAuth client id which is normally email ,

**code** (integer): http status codes like 200 for success ,

**error** (string): Have value if code is not 200, it provides the complete details about the error occured ,

**message** (string, optional): Message details in case of success or failure ,

**path** (string): URL for the invoked http resource ,

**refreshToken** (string): represents the oAuth refresh token ,

**timestamp** (Timestamp, optional): Represents current timestamp

**}**

**Timestamp {**

date (integer, optional),

day (integer, optional),

hours (integer, optional),

minutes (integer, optional),

month (integer, optional),

nanos (integer, optional),

seconds (integer, optional),

time (integer, optional),

timezoneOffset (integer, optional),

year (integer, optional)

**}**

**Sample response**

{

"code": 200,

"error": "",

"timestamp": "2019-07-11T11:34:05.116+0000",

"message": "",

"path": "/ns/api/v1/auth/get/accesstoken",

"accessToken": "b6a29ed0f4174032bd991892021cc1ee",

"refreshToken": "cb53d097c5d742ce983dbf81a5011ee4",

"authorizeToken": null,

"clientId": "test"

}

### Get Refresh Token

The Refresh Token grant type is used by clients to exchange a refresh token for an access token when the access token has expired.

This allows clients to continue to have a valid access token without further interaction with the user.

**HTTP Method:** POST

**URL:** POST /ns/api/v1/auth/get/refreshtoken

**Request Headers**

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Type | Required/Optional | Description |
| **clientId** | String | Required | Its unique id normally representing email |
| **refreshToken** | String | Required | Represents Refresh Token, for which you will get the new access token |

#### Response

**AuthResponseDTO {**

**accessToken** (string): represents the oAuth access token ,

**authorizeToken** (string, optional): represents the oAuth authorize token ,

**clientId** (string): represents the oAuth client id which is normally email ,

**code** (integer): http status codes like 200 for success ,

**error** (string): Have value if code is not 200, it provides the complete details about the error occured ,

**message** (string, optional): Message details in case of success or failure ,

**path** (string): URL for the invoked http resource ,

**refreshToken** (string): represents the oAuth refresh token ,

**timestamp** (Timestamp, optional): Represents current timestamp

**}**

**Timestamp {**

date (integer, optional),

day (integer, optional),

hours (integer, optional),

minutes (integer, optional),

month (integer, optional),

nanos (integer, optional),

seconds (integer, optional),

time (integer, optional),

timezoneOffset (integer, optional),

year (integer, optional)

**}**

**Sample response**

{

"code": 200,

"error": "",

"timestamp": "2019-07-11T11:34:05.116+0000",

"message": "",

"path": "/ns/api/v1/auth/get/ refreshtoken",

"accessToken": "b6a29ed0f4174032bd991892021cc1ee",

"refreshToken": "cb53d097c5d742ce983dbf81a5011ee4",

"authorizeToken": null,

"clientId": "test"

}