

Cygnet fame enriched API Specification

This document contains api specification to access functionalities of cygnet fame

Cygnet Infotech

**Version History**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Version** | **Prepared By** | **Prepared On** | **Reviewed & Approved By** | **Reviewed & Approved On** | **Description** |
| 1.0 | Parth Doshi | 03-07-2019 | Fenil Rathod | 03-07-2019 | Initial Draft. |
| 1.1 | Amit Khanna | 03-07-2019 | Fenil Rathod | 03-07-2019 | Initial Draft. |
| 1.2 | Parth Doshi | 26-08-2019 | Rajesh Khunt | 26-08-2019 | Updated data encryption steps. |
| 1.3 | Sagar Sathwara | 23-08-2023 | Darshit Gajjar | 24-08-2023 | Added Encryption Decruption Flag |

Table of Contents

[API Overview 3](#_Toc37337278)

[API Format 3](#_Toc37337279)

[API Request Headers 3](#_Toc37337280)

[Sample Encrypted Request JSON 4](#_Toc37337281)

[App\_Key Overview 4](#_Toc37337282)

[API Request Overview 5](#_Toc37337283)

[API Response Overview 5](#_Toc37337284)

[Error Payload 6](#_Toc37337285)

[Response HTTP Status Code 6](#_Toc37337286)

[Common Error Codes 6](#_Toc37337287)

[API List 7](#_Toc37337288)

[Authentication 7](#_Toc37337289)

# API Overview

## API Format

APIs will be published as stateless REST endpoints over HTTPS. Below table describes the URI pattern to be used while consuming API end points:

|  |  |
| --- | --- |
| API URI | https://{domain-name}/{api-group}/{version}/{url-segment} |
| Http Method | Get – To fetch the data  Post – To submit the data |
| Content Type | application/json, text/plain |
| URL Description | |
| https | All API will be published through HTTPS channel only. Same protocol will be used in no-production environments |
| Domain-name | Domain name of the API Gateway.  **Staging (sandbox)**  [https://staging-enrichedapi.cygnetfame.in](https://staging-enrichedapi.cygnetfame.in/)  **Production**  [https://enrichedapi.cygnetfame.in](https://staging-enrichedapi.cygnetfame.in/) |
| API Group | This is the optional url part. It is being used to group the API endpoints. |
| Version | Version of the published API. Version number will be prefixed by “v” and is always mandatory. E.g. v0.1 |
| URL-Segment | Rest part of the URI should be ending point name and parameters to call the API |

## API Request Headers

All Cygnet FAME API requests require the following http headers except auth-token API. All http headers are mandatory.

|  |  |  |
| --- | --- | --- |
| **Headers** | | **Sample Value** |
| Content-Type | application/json |  |
| clientid | {{client id provided by Cygnet GSP}} | 1mg6hEi+9VXVkQ7bDC0QxEkVmiFhnm/lc6XG3ENZrn2MgWlJUCZF7c6LIUELoFoWt8F4QAbqPbGTgTg6FrqGGI+1ClDnnHRwvfeaeceBqSluiENNG+mXpI/1MjRmm5xC |
| client-secret | {{client secret provided by Cygnet GSP}} | qn85jt7FLStqnccLeHwY/vKuFAAn2EghMdVbC/zWxfeNzwl0Nq0Sq96/6wWwxJu8xvfC91jga/IZZo6ZzGWdFudGIILPKcybFJfXEkTQJr29ca+Udr+2N5aJZpB4Y2+cO94NshH9sMe2XhresKum7siVRCJOXJzHshq4T4Q9XFhjBfYzJn6M8TH3PvkFSHZGObj1pJ/2xDA+2d3CZ+Z2qPdjzzAh09cVowLVWWk3CtOjbUr73j7etsaPumelO/KG |
| txn | {{unique random alpha-numeric string}}  Max Length: 40 | CYG201904ASD234ARER |
| ip-usr | {{ip-address}}  Max Length: 40  127.0.0.1 can be passed as default if don’t want to pass actual ip address. | 127.0.0.1 |
| auth-token | {{auth-token}} retrieved using authentication API | a8a924e468a6d5e03e76dfad2d2fb07157ee0fda0688139ae49aab01854ec598 |
| IsEncryptionRequired | {string value} | “true” or “false” |

## Sample Encrypted Request JSON

All Cygnet FAME API request body accepts only encrypted json payload. Below is sample data attributed with encrypted json payload.

|  |
| --- |
| **Encrypted Request JSON** |
| {  "**data**": ""  } |

## App\_Key Overview

App\_key is used to encrypt and decrypt the request and response post authentication API. **It is 256 bit random AES key**.

API consumer needs to create such key during authentication and to use same key afterwards to encrypt the request and to decrypt the response.

The same key will be used by API gateway to decrypt the request and to encrypt the response.

So, steps will be:

1. Generate AES key.
2. Base64 encoding of JSON data.
3. Encrypt encoded base64 JSON data using AES key.
4. Base64 encoding of the above encrypted data.
5. Base64 encoding of AES key.
6. Encrypt encoded base64 AES key with Cygnet GSP RSA public key.
7. Base64 encoding of the above encrypted key.
8. Decrypt data received from enriched API using your AES key.
9. Base64 Decode of decrypted data.

## API Request Overview

Generate AES key using AesCryptoServiceProvider with Mode = ECB, Padding = PKCS7, KeySize = 256 & BlockSize = 128.

Using this key, you need to encrypt base64 encoded JSON data which you need to pass to API. So, your encrypted base64 encoded data will look like below:

**{"data":"vqNU4xIzqu5SM8UQbdOc+rs5nSKFp83mHTb4bKkqGhb50VWILHo/YVvW++"}**

Now, first you need to encode this AES key into base64 format. Encrypt this base64 encoded AES key using RSA public key of Cygnet GSP. Your encrypted base64 encoded AES key would like below:

**{"app\_key": "QF37oTyQLOUYzmDm3l9BPUuz6ObvrEgNcAHbeR/Oga5Zg873Qxk6GmKi1A=="}**

So finally, API call will look like

**{"data": "vqNU4xIzqu5SM8UQbdOcR899VCiLT/p83mHTb4bKkqGhb50VWILHo/YVvW++","app\_key": mSc4wAyNKQtnnn3d1xJNrDhNXLjKGQxk6GmKi1A=="}**

## API Response Overview

In general, you will receive response like below:

{

"data": "Uhh8WZsnh8HG26RJiyIaie3eBALYSew+Y141+i12I8sEKbzpwaehpgRZD8jPgECxjOeswfN4wpeduv+iAyXFXKC1rFdjsxVZ6lNkQg17u13YTUowqvf9UcYoCaH4xjyhhHffHs60jrfeAql50pSb5YP2UhnDtSsK2Iv/t59NrIhCUujW7RrNAlZGQkw+Yh+V",

"status\_cd": 1

}

To decrypt data your received from response, you need to use same AES key which you have used during authentication API call. Perform Base64 decoding on decrypted data to have response in plain format.

## Error Payload

{

“status\_cd” : “0”,

error: {

“error\_cd” : “error code”,

“message” : “customized error message”

}

}

## Response HTTP Status Code

|  |  |
| --- | --- |
| 200 | Successful response. To be used when request is processed successfully. |
| 400 | Bad Request. When system detects issue in the input data. |
| 401 | Unauthorized. When system detects access to resource which is not authorized. |
| 404 | Not Found. If requested API is not found. |
| 405 | Method not found. If requested HTTP Method is not available. |
| 500 | Exception. If system fails to process request due to exceptions in the system |

## Common Error Codes

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Error Code** | **HttpStatusCode** | **Description** |
| 1 | UNK0001 | 500 | Unknown or technical error. |
| 2 | AUTH0001 | 401 | Authentication failed. Passed CilentId, Client-Secret or Authentication Token is invalid. |
| 3 | AUTH0002 | 401 | Authorization failed. User is not authorized to perform requested operation. |
| 4 | AUTH0003 | 409 | API Limit Over. API request throttling rate reached over defined limit. |
| 5 | AUTH0004 | 400 | Missing API header parameters or its value. |
| 6 | AUTH0005 | 503 | API access blocked. |
| 7 | AUTH0006 | 400 | Api request payload size exceeded. |

# API List

## Authentication

Authentication API needs to be called first to acquire auth-token and to pass app\_key. All subsequent APIs will be accessible using auth-token only. And encryption and decryption will be work on passed app\_key only.

|  |  |
| --- | --- |
| API Overview | |
| URL | [https://<<domain-name>>/v0.1/authenticate/token](https://qa-enrichedapi.cygnetgsp.in/v0.1/authenticate/token) |
| Type | POST |

|  |  |
| --- | --- |
| Sample Request Json | |
| data | {  "data": {  "username": "demo.user@cygnetinfotech.com",  "password": "Admin@123"  },  "app\_key": "iDCzcm9FuhtRRbMQkdpnYBVbUiJR+0sd670ejpbsOWBexwSCO99JY88isrpqVAU1zw3/AJrkTbHOgvlOs9+ZWe1OtxIccX+PUr2dQdFCJz3u2+2+8ope3i1UOuVHgdj0PxUjQb+tEouciMbDECM6f16UfTxSBwyHBu9jKMqxhd7WO4P4PEXQPQfS1Zui+ZBGinDUd24DQp/3HComrokIZqbHPXZlcl58qNebWDOGUcX/vwRgKGvlRgvsyDNPG9DbWOAL3B/578IF8jh+zoS631lR3nUqVEjMGxcgZDM4jQTARLlywxkZxBZDGTlfWhcjrBtcVDD7PoZG4NH2nIR4fw=="  } |

|  |
| --- |
| Encrypted Request Payload |
| {  "**data**": "dsDCgys2hVbVm7cMQbKwEDwZyjcD7mJnZ43wXDM0Hy+VgS3X5IYf5R7/2j2DHJNwc93MZ5flWS3kM9YZ2Fdumrz/N+l4EhB7KOUSNP69JJ+318mnLD9x3i117itvhdIagznSTEWSyXBI62nykygIPg==",  "**app\_key**": "VuvDyKRagUXBXC2Ikdx73RfVqrKJoKOHP/GSEhqU+NWasCwP/+5kE/4RM1siW5PosrJFDjQsjqPu3APzTTR8w4At50icADn+bebTZqs1srn1RP4lxgMIdxRg68EEAZ3oGD8NrytWlLYZHiwx5wVE1F91A7+PitvwK71boHfVCRxCaECqRz2/P+RSJDk2kusVZokFMcHI0Ute+6cqjhnRrbMtpS2z284wziDspKJ4zZMl1Ms2aPgemt6TvYnRHMH/jaAjRZ8BivD38qBs6NeD06u2DrD+ni4UDiJJ2AmbNvH8ui0SLU3K5EbzfbW72W05aQj3hZqpM97ZVAJuXaTDZg=="  } |

|  |
| --- |
| Without Encrypted Request Payload(Base64) |
| {  "**data**": "",  "**app\_key**": "iDCzcm9FuhtRRbMQkdpnYBVbUiJR+0sd670ejpbsOWBexwSCO99JY88isrpqVAU1zw3/AJrkTbHOgvlOs9+ZWe1OtxIccX+PUr2dQdFCJz3u2+2+8ope3i1UOuVHgdj0PxUjQb+tEouciMbDECM6f16UfTxSBwyHBu9jKMqxhd7WO4P4PEXQPQfS1Zui+ZBGinDUd24DQp/3HComrokIZqbHPXZlcl58qNebWDOGUcX/vwRgKGvlRgvsyDNPG9DbWOAL3B/578IF8jh+zoS631lR3nUqVEjMGxcgZDM4jQTARLlywxkZxBZDGTlfWhcjrBtcVDD7PoZG4NH2nIR4fw=="  } |

|  |
| --- |
| Response Payload |
| {  "**data**": "4gfnGc0PVEZs5rPQojn9tZ2u8Gk+LuWoSyLYy2MWe1MfGylI2i7f9gv7zmFBjrYeOVpxVcqcvPEgsvAmkXSADWh2c5v+NXUMccGl05xirXpoSRxhE2EpQNLKUL2mwcbv7f2lkomP0ZKqvoyA4QQuv8a8LA178vqmApH2332itKnxiEbR6N/9ASUKV4DfkmAl",  "**status\_cd**": 1  } |

|  |
| --- |
| Without Encrypted Response Payload(Base64) |
| {  "**data**":"  eyJhdXRoLXRva2VuIjoiYzU2NjkwNzJiNTVmZDUyZDVkM2IxYzg2NGUyMzE0NzZkOTIwZDAwZDRkZjA0Zjk5ZjdjODVhNWI5YmY5ZDU2ZiIsImV4cGlyeSI6MzYwfQ==",  "**status\_cd**":1  } |

|  |
| --- |
| Decrypted Response Payload |
| {  "**auth-token**": "68f123a2fb7a5126b19c76870850135a4b1cf9ca3c3087ebf765d61f289846d4",  "**expiry**": 360  } |

#### Attribute Details

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Field | Description | Type | Max Length | Required |
| username | User Name | String | 64 | Yes |
| Password | Password | String | 64 | Yes |

#### Error Codes

|  |  |  |
| --- | --- | --- |
| Error Codes | Error Message | |
| E050 | | Sorry, your email or password is incorrect. |
| E001 | | Unknown error occurred. |