Know Your Customer

API User Guide 2024

by Know Your Customer

Last updated: 18 Nov 2022

Know Your Customer

Table of Content

Glossary & Reference

Term	Description
Full KYC case	An entity case for which complete company structure is built, mandatory documents are obtained and AML check is performed by the KYC system. An individual case for which mandatory documents are obtained and verified, AML check is performed by the KYC system.
Manual Case	This is a case which is created as an unregistered entity case or without live registry connection.
AML	Anti-money laundering.
AML only case	An individual/entity case for which only AML check is completed by KYC app.
User	Any authorized user of a KYC API endpoint.
End-user	Any customer of KYC's clients.
casecommonID	Unique identifier allocated by the KYC system to a case.
casestepID	Unique identifier allocated by the KYC system to a step.
Deactivated Steps	A step would have Deactivated state based on the following conditions: • Based on your company's preferences, controlling bodies that must have ID verification performed would be in activated state. The steps that are deactivated (isDeactivated = 'true') have been screened against AML and Sanctions lists and are clear of any matches. These steps may not require full KYC verification. • Shareholder steps that are deactivated (isDeactivated = 'true') are the minority shareholders with less than your configured shareholding threshold and qualify for simplified due diligence. They have been screened against AML and Sanctions lists and are clear of any matches. Where required a deactivated step can be activated for full KYC verification.

1. KYC API tech documentation

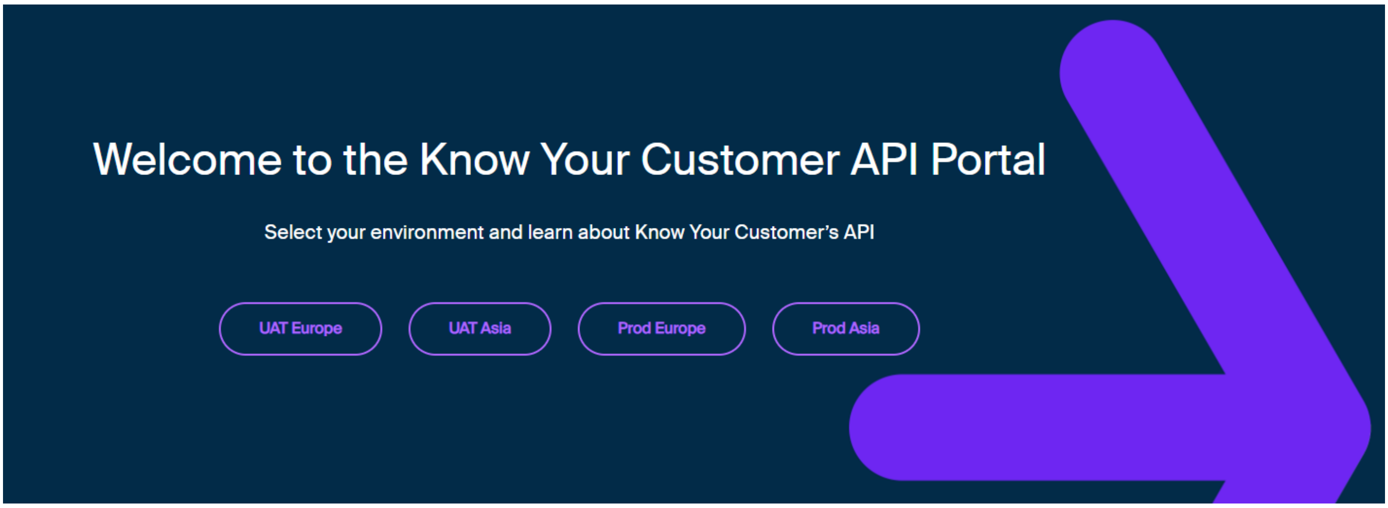
2. Information on obtaining key inputs for endpoints described in this document

   a. How to get casecommonId?
      - *casecommonID* is returned when a case is created
      - *casecommonID* of company case can be obtained by browsing case list using GET Companies endpoint #/Companies/get_v2_Companies
      - *casecommonID* of Individual case can be obtained by browsing case list using GET Individuals endpoint #/Individuals/get_v2_Individuals

   b. How to get casestepID?
      - *casestepID* of Individual/entity case can be obtained from GET Case steps endpoint #/CaseSteps/get_v2_CaseSteps_caseCommonId_

1.0 Navigating the KYC API Portal

The KYC API Portal is accessible from https://knowyourcustomer.com/api/



Welcome to the Know Your Customer API Portal

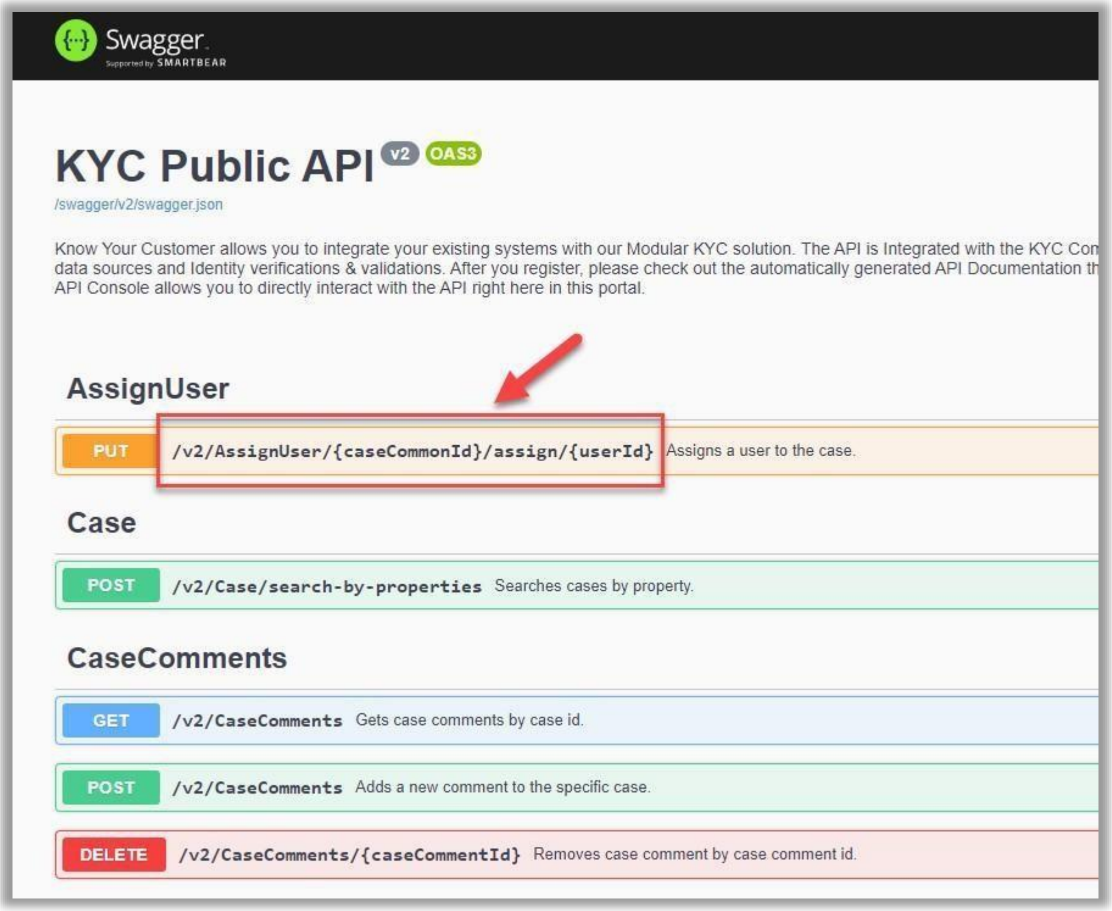
Select your environment and learn about Know Your Customer's API

The portal gives users access to 4 different environments to choose from based on their requirements. Users should choose the index page that applies to them between the User Acceptance Testing (UAT) and Production environments in either Europe or Asia.

#	Environment	Direct Link to index page
1	UAT Europe	https://api-uat.knowyourcustomer.com/swagger/index.html
2	UAT Asia	https://api-uathk.knowyourcustomer.com/swagger/index.html
3	Production Europe	https://api.knowyourcustomer.com/swagger/index.html
4	Production Asia	https://api-asia.knowyourcustomer.com/swagger/index.html

Note:

1. All the methods described in this document are for accessing KYC Public API v2.



KYC Public API v2 OAS3

/swagger/v2/swagger.json

Know Your Customer allows you to integrate your existing systems with our Modular KYC solution. The API is Integrated with the KYC Con
data sources and Identity verifications & validations. After you register, please check out the automatically generated API Documentation th
API Console allows you to directly interact with the API right here in this portal.

AssignUser

PUT /v2/AssignUser/{caseCommonId}/assign/{userId} Assigns a user to the case.

Case

POST /v2/Case/search-by-properties Searches cases by property.

CaseComments

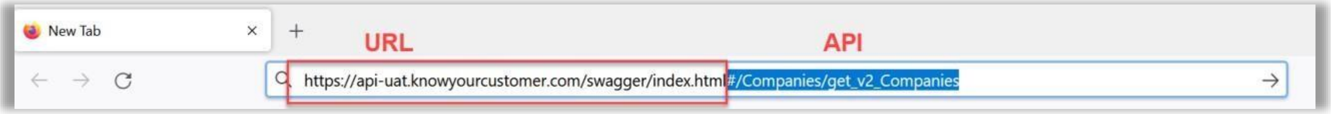
GET /v2/CaseComments Gets case comments by case id.

POST /v2/CaseComments Adds a new comment to the specific case.

DELETE /v2/CaseComments/{caseCommentId} Removes case comment by case comment id.

2. The methods detailed in this document can be accessed by adding the specific string to the relevant environment URLs as listed on p.4.

   For example, to access the GET Companies List endpoint in the UAT Europe environment, add #/Companies/get_v2_Companies to the URL as follows: https://api-uat.knowyourcustomer.com/swagger/index.html#/Companies/get_v2_Companies



https://api-uat.knowyourcustomer.com/swagger/index.html#/Companies/get_v2_Companies

   Similarly, if you are connecting to production, add #/Companies/get_v2_Companies_ to the Production URL as follows: https://api.knowyourcustomer.com/swagger/index.html#/Companies/get_v2_Companie

2.0 Bearer token authentication

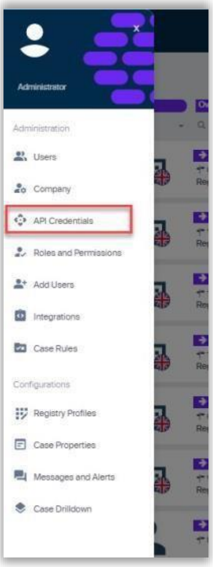
KYC API endpoints can be accessed by supplying the bearer key generated on the Know Your Customer platform for the client id. Multiple secret keys can be added for each client id.

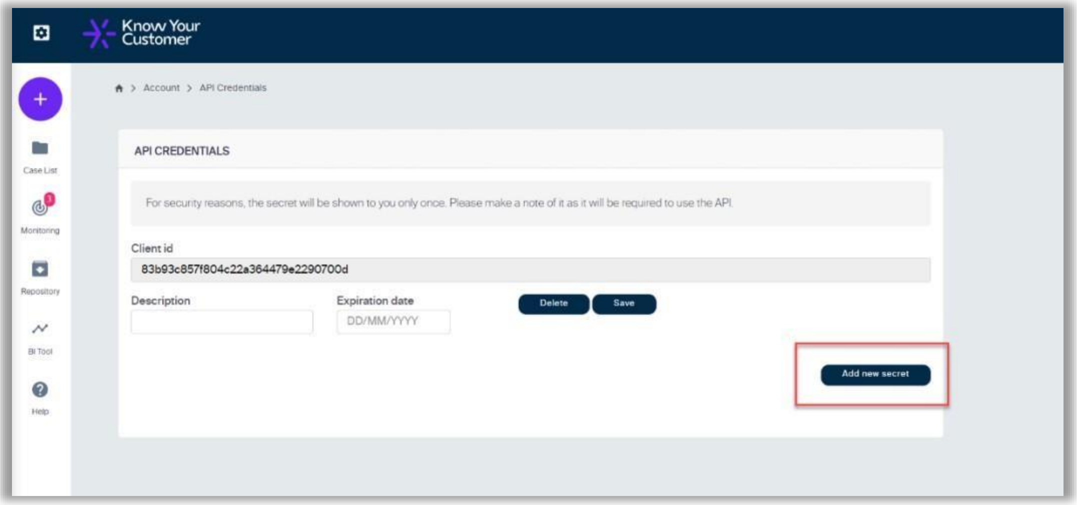
Prerequisite

Administrator access to the platform is required to get the secret key. If you don't have administrator access, please contact KYC support at help@knowyourcustomer.com

1. Steps to get secret key

1. Log in to Know Your Customer with administrator credentials
2. Under the menu items accessible from the gear icon in the top left corner, select Administration >> API Credentials





API CREDENTIALS

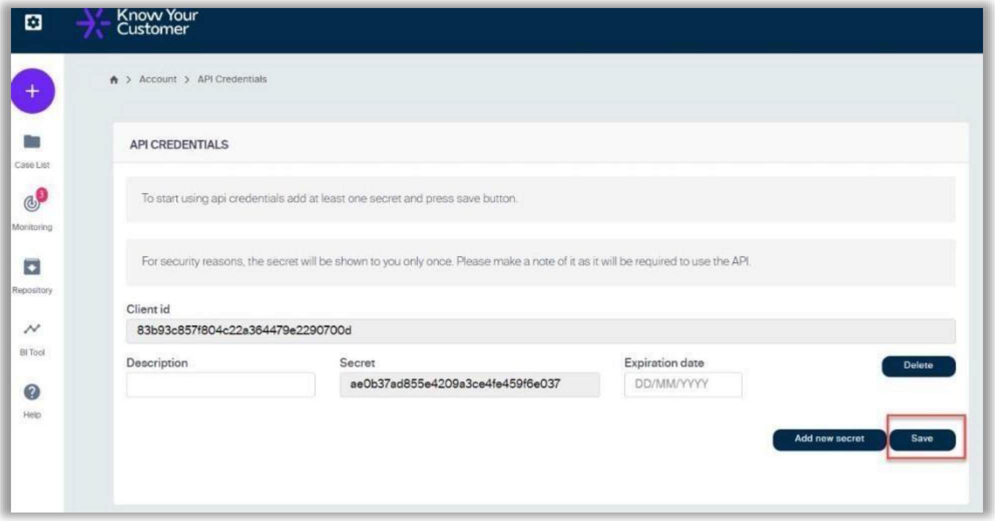
For security reasons, the secret will be shown to you only once. Please make a note of it as it will be required to use the API.

Client id: 83b93c857f804c22a364479e2290700d

Description:

Expiration date: DD/MM/YYYY

3. A new secret key can be added by clicking "Add new secret button"



API CREDENTIALS

To start using api credentials add at least one secret and press save button.

For security reasons, the secret will be shown to you only once. Please make a note of it as it will be required to use the API.

Client id: 83b93c857f804c22a364479e2290700d

Description:

Secret: ae0b37ad855e4209a3ce4fe459f6e037

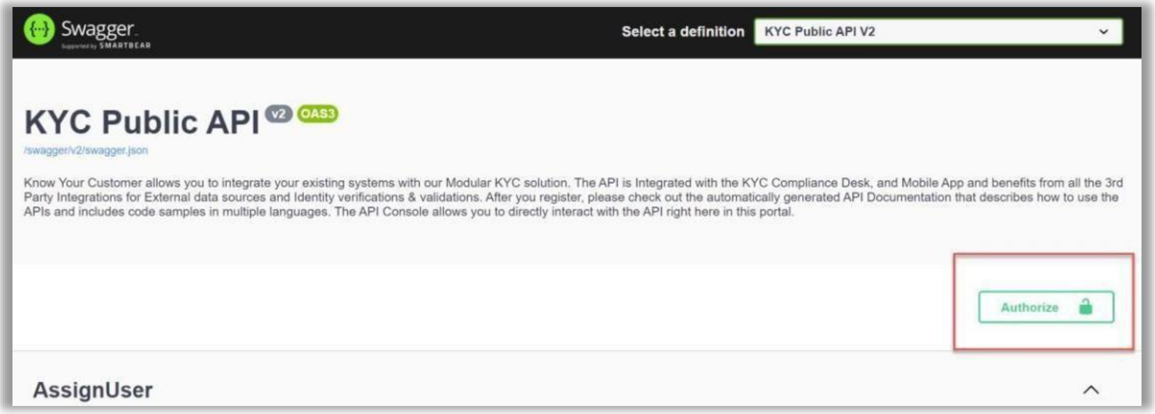
Expiration date: DD/MM/YYYY

4. Once the secret is generated, user should save the secret key by clicking the Save button. User can add a description and an expiry date before saving the secret.
5. For security reasons, the secret key will be shown to the user only once. Please make a note of it as it will be required to use the API

2. Steps to authorize user on API portal

Note: For security purposes, the bearer token expires after 10 minutes from the time it is generated.

1. Click on the Authorize button

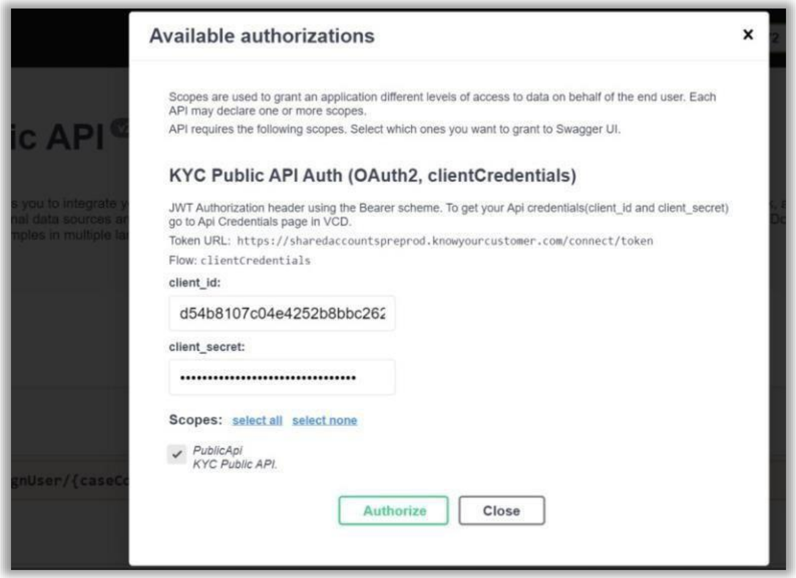


KYC Public API

/swagger/v2/swagger.json

Know Your Customer allows you to integrate your existing systems with our Modular KYC solution. The API is Integrated with the KYC Compliance Desk, and Mobile App and benefits from all the 3rd Party Integrations for External data sources and Identity verifications & validations. After you register, please check out the automatically generated API Documentation that describes how to use the APIs and includes code samples in multiple languages. The API Console allows you to directly interact with the API right here in this portal.

2. Enter the client id and client secret code obtained from the KYC platform. Make sure the PublicApi option is checked in the Scopes section.



Scopes are used to grant an application different levels of access to data on behalf of the end user. Each API may declare one or more scopes.

API requires the following scopes. Select which ones you want to grant to Swagger UI.

KYC Public API Auth (OAuth2, clientCredentials)

JWT Authorization header using the Bearer scheme. To get your Api credentials(client_id and client_secret) go to Api Credentials page in VCD.

Token URL: `https://sharedaccountspreprod.knowyourcustomer.com/connect/token`

Flow: `clientCredentials`

client_id: d54b8107c04e4252b8bbc262

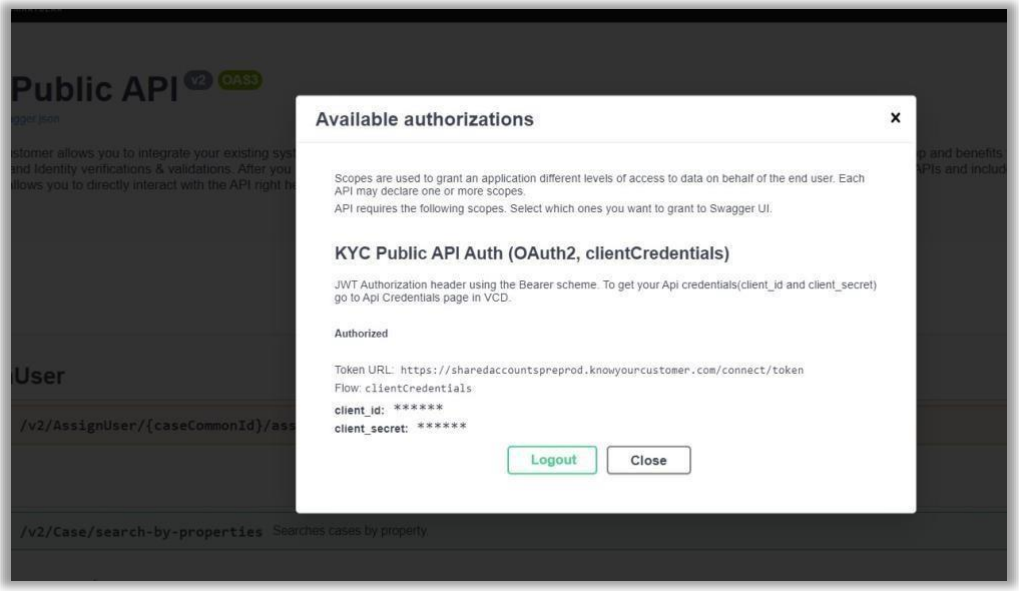
client_secret: ••••••••••••••••••••••••••••••••

Scopes: select all select none

☑ *PublicApi*
KYC Public API.

3. Click the Authorize button.

4. Once authorized successfully, user can access the API endpoints.



Available authorizations

Scopes are used to grant an application different levels of access to data on behalf of the end user. Each API may declare one or more scopes.

API requires the following scopes. Select which ones you want to grant to Swagger UI.

KYC Public API Auth (OAuth2, clientCredentials)

JWT Authorization header using the Bearer scheme. To get your Api credentials(client_id and client_secret) go to Api Credentials page in VCD.

Authorized

Token URL: `https://sharedaccountspreprod.knowyourcustomer.com/connect/token`

Flow: `clientCredentials`

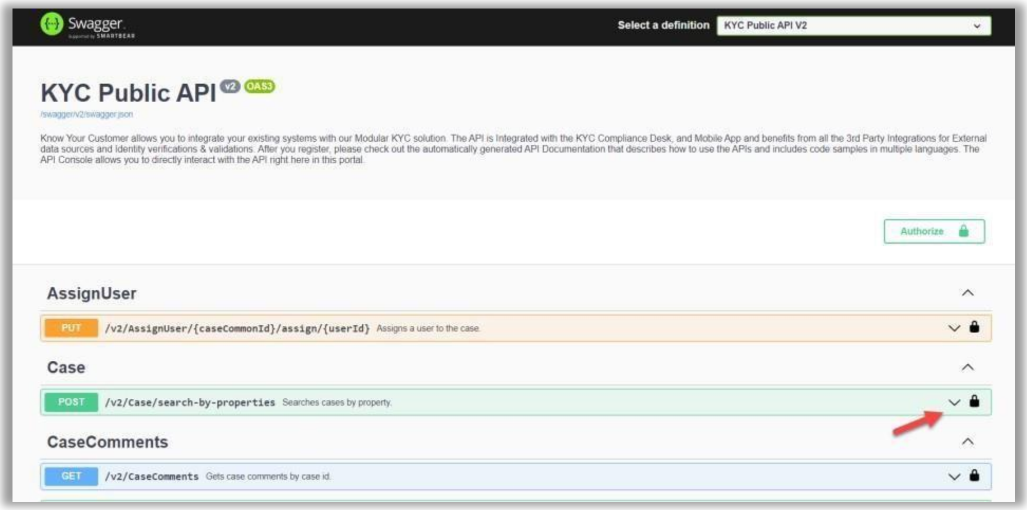
client_id: ******

client_secret: ******

Public API
v2
OAS3
User
/v2/AssignUser/{caseCommonId}/ass
/v2/Case/search-by-properties
Searches cases by property.
×
Logout
Close

3. Access API endpoints after authorization

1. To access the endpoint, go to the required endpoint on the page
2. Click expand menu to view the options available for the endpoint

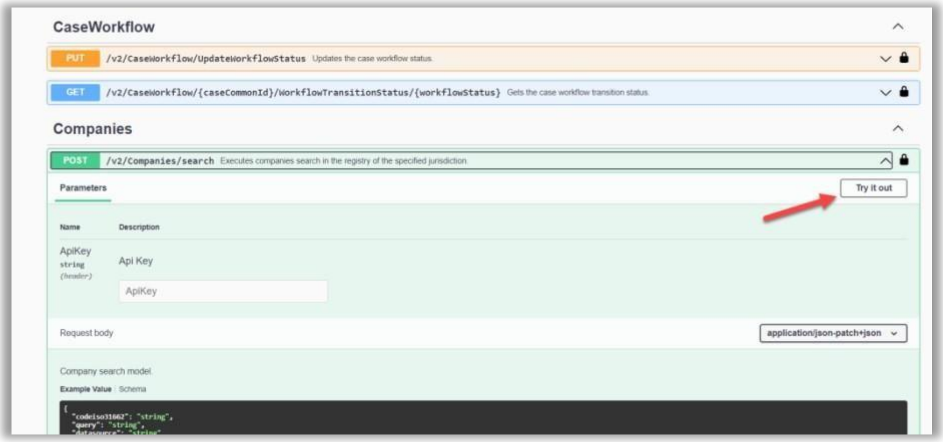


Know Your Customer allows you to integrate your existing systems with our Modular KYC solution. The API is Integrated with the KYC Compliance Desk, and Mobile App and benefits from all the 3rd Party Integrations for External data sources and Identity verifications & validations. After you register, please check out the automatically generated API Documentation that describes how to use the APIs and includes code samples in multiple languages. The API Console allows you to directly interact with the API right here in this portal.

Select a definition: KYC Public API V2

Swagger
Supported by SMARTBEAR
KYC Public API
v2
OAS3
/swagger/v2/swagger.json
Authorize
AssignUser
PUT
/v2/AssignUser/{caseCommonId}/assign/{userId}
Assigns a user to the case.
Case
POST
/v2/Case/search-by-properties
Searches cases by property.
CaseComments
GET
/v2/CaseComments
Gets case comments by case id.

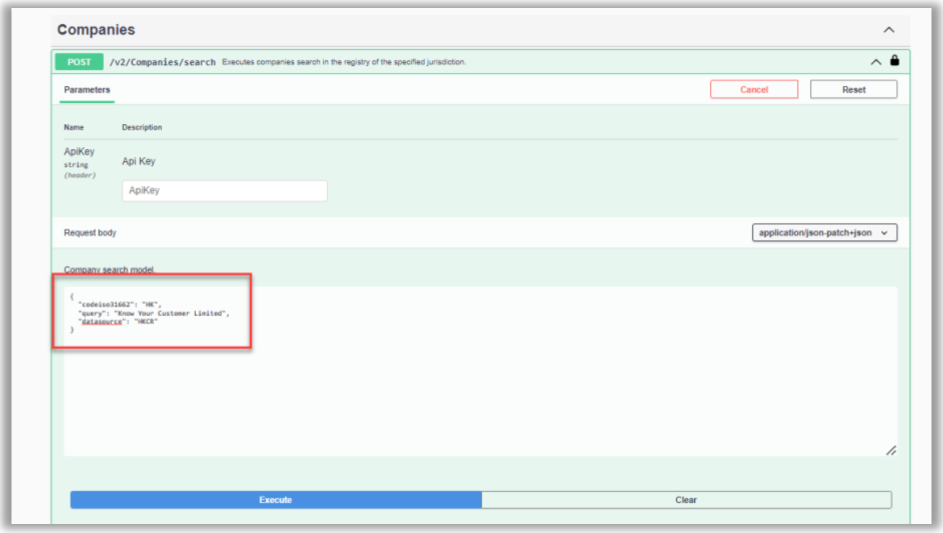
3. Click “**Try it Out**” button



CaseWorkflow
PUT
/v2/CaseWorkflow/UpdateWorkflowStatus
Updates the case workflow status.
GET
/v2/CaseWorkflow/{caseCommonId}/WorkflowTransitionStatus/{workflowStatus}
Gets the case workflow transition status.
Companies
POST
/v2/Companies/search
Executes companies search in the registry of the specified jurisdiction.
Parameters
Try it out
Name
Description
ApiKey
string
(header)
Api Key
ApiKey
Request body
application/json-patch+json
Company search model.
Example Value
Schema

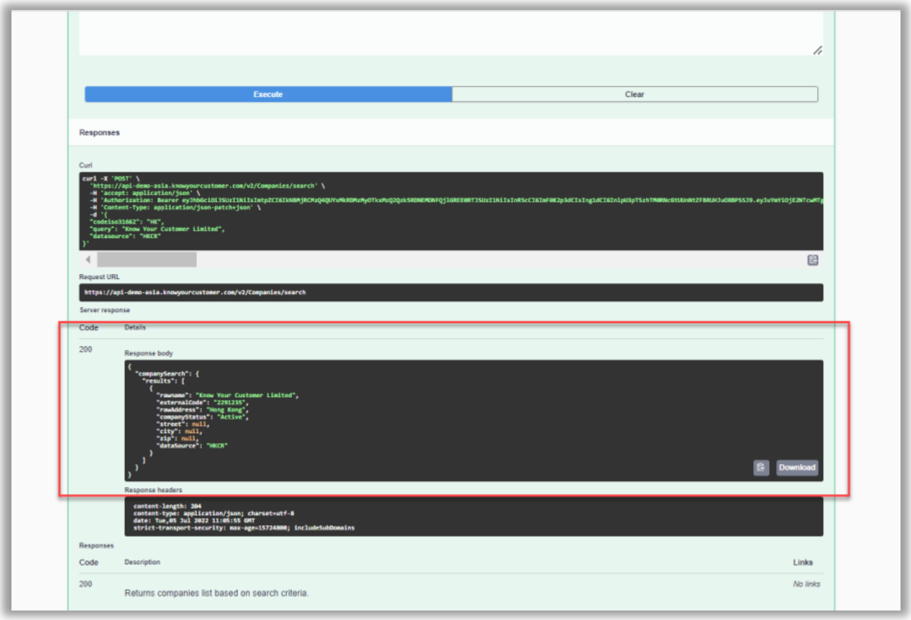
```
{
  "codeiso31662": "string",
  "query": "string",
  "datasource": "string"
```

4. Enter the parameters and click “Execute”



```
{
  "codeiso31662": "HK",
  "query": "Know Your Customer Limited",
  "datasource": "HKCR"
}
```

5. The endpoint returns the response for the request



```
curl -X 'POST' \
  'https://api-demo-asia.knowyourcustomer.com/v2/Companies/search' \
  -H 'accept: application/json' \
  -H 'Authorization: Bearer eyJhbGciOiJSUzI1NiIsImtpZCI6IkNBMjRCMzQ4QUYxMkRDMzMyOTkxMzQ2Qzk5RDNEMDNFQjlGREE0RTJSUzI1NiIsInR5cCI6ImF0K2p3dCIsIng1dCI6InlpU3pTSzhTM0RNcGtUUnNtZFBRUHJuOXBPS5J9.eyJuYmYiOjE2NTcwMTg
  -H 'Content-Type: application/json-patch+json' \
  -d '{
  "codeiso31662": "HK",
  "query": "Know Your Customer Limited",
  "datasource": "HKCR"
}'
```

Request URL

```
https://api-demo-asia.knowyourcustomer.com/v2/Companies/search
```

Server response

Code	Details
200	Response body

```
{
  "companySearch": {
    "results": [
      {
        "rawname": "Know Your Customer Limited",
        "externalCode": "2291235",
        "rawAddress": "Hong Kong",
        "companyStatus": "Active",
        "street": null,
        "city": null,
        "zip": null,
        "dataSource": "HKCR"
      }
    ]
  }
}
```

Response headers

```
content-length: 204
content-type: application/json; charset=utf-8
date: Tue,05 Jul 2022 11:05:55 GMT
strict-transport-security: max-age=15724800; includeSubDomains
```

Responses

Code	Description	Links
200	Returns companies list based on search criteria.	*No links*

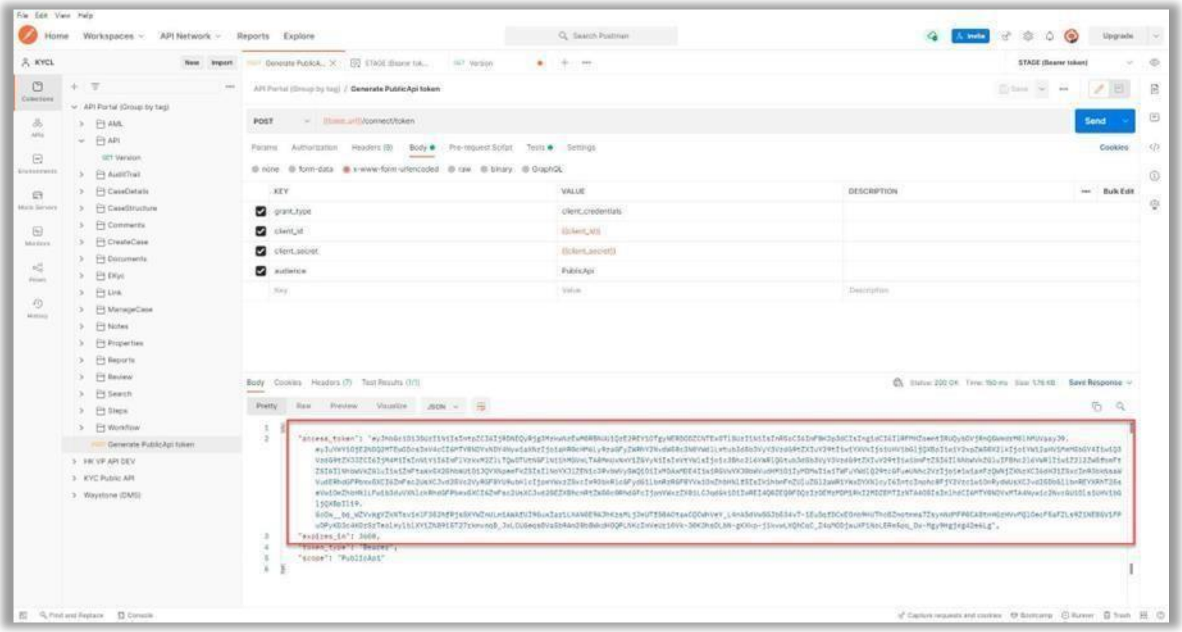
4. Authorization expiry

4.1 API Portal

1. Once authorized with the Client ID and Client secret key, the API portal session shall be valid for 1 hour
2. Every hour the user has to reauthorize the session by following the steps as described in point 2 of section 2.0.2

4.2 Http Request

1. The API portal authorization token can be obtained by passing the following parameters via ‘Generate PublicApi token’ endpoint
    1. servicegrant_type=client_credentials
    2. client_id=”YOUR_CLIENT_ID”
    3. client_secret=”YOUR_CLIENT_SECRET”
    4. audience=PublicApi
2. The service then returns the authorization code that should be used with the bearer authentication for each API request
3. On authorization expiry, user can request for reauthorization via Generate PublicApi token endpoint using steps as described above



API Portal (Group by tag) / Generate PublicApi token

POST {{base_url}}/connect/token

○ none ○ form-data ● x-www-form-urlencoded ○ raw ○ binary ○ GraphQL

	KEY	VALUE	DESCRIPTION
☑	grant_type	client_credentials	
☑	client_id	{{client_id}}	
☑	client_secret	{{client_secret}}	
☑	audience	PublicApi	
	Key	Value	Description

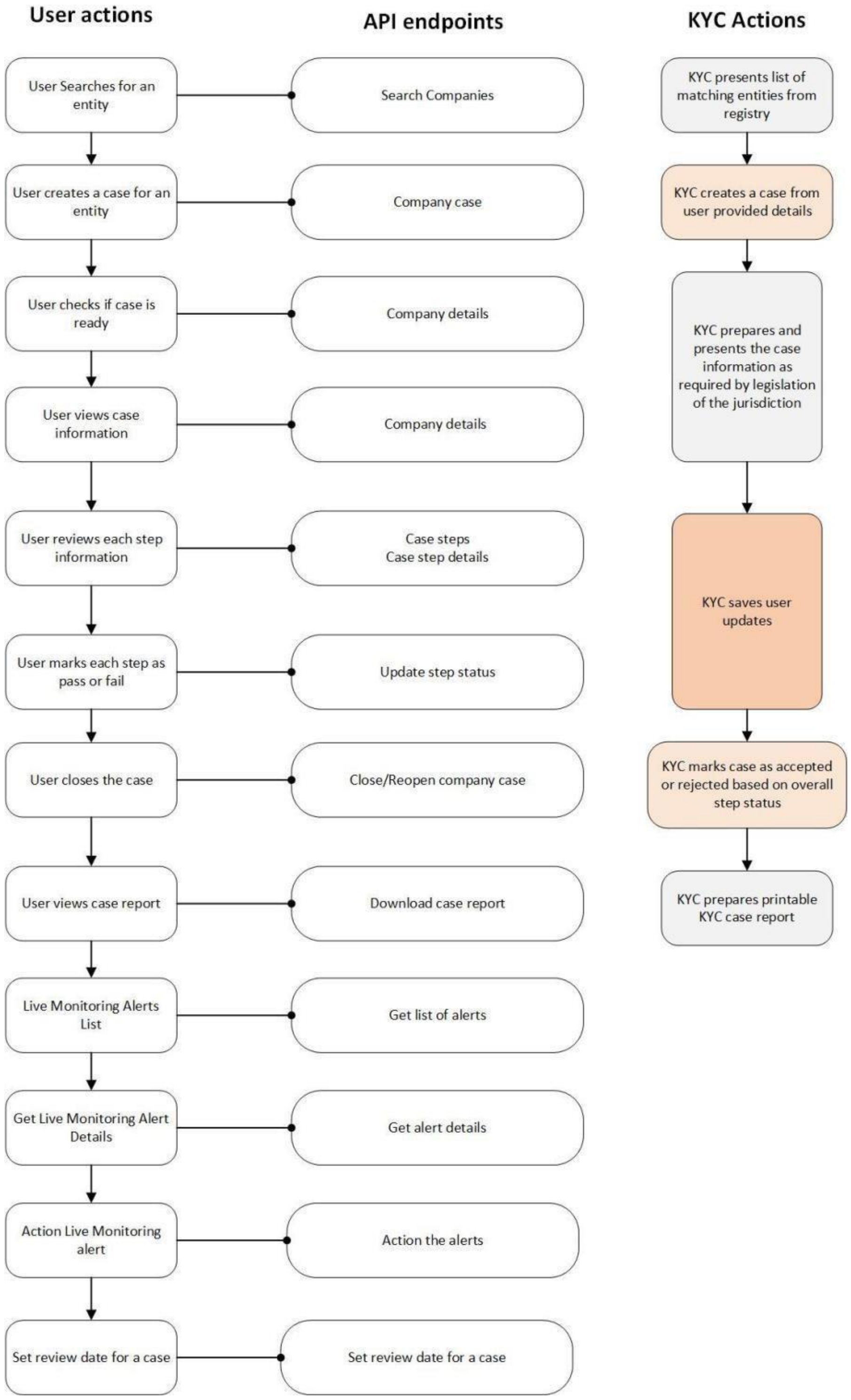
```
{
    "access_token": "[illegible]",
    "expires_in": 3600,
    "token_type": "Bearer",
    "scope": "PublicApi"
}
```

4.3 Code example to build "Authorization" header in generate token request

```
var encoding = Encoding.GetEncoding("iso-8859-1");
var clientId = "xxx";
var secret = "xxxx";
var toEncode = clientId + ":" + secret;
var baseEncoded = Convert.ToBase64String(encoding.GetBytes(toEncode));
var header = "Basic " + baseEncoded;
```

3.0 Entity Case

Please see below a usual flow of user interaction with Know Your Customer when preparing a compliance case for a corporate entity.


User actions
API endpoints
KYC Actions
User Searches for an entity
Search Companies
KYC presents list of matching entities from registry
User creates a case for an entity
Company case
KYC creates a case from user provided details
User checks if case is ready
Company details
KYC prepares and presents the case information as required by legislation of the jurisdiction
User views case information
Company details
User reviews each step information
Case steps
Case step details
KYC saves user updates
User marks each step as pass or fail
Update step status
User closes the case
Close/Reopen company case
KYC marks case as accepted or rejected based on overall step status
User views case report
Download case report
KYC prepares printable KYC case report
Live Monitoring Alerts List
Get list of alerts
Get Live Monitoring Alert Details
Get alert details
Action Live Monitoring alert
Action the alerts
Set review date for a case
Set review date for a case

The next section provides a detailed breakdown of each step of a user's interaction with the Know Your Customer system for entity cases.

3.1 Search for an entity

API endpoint:

#	API endpoint	Method
1	Companies Search	#/Companies/post_v2_Companies_search
2	Jurisdictions	#/Jurisdictions/get_v2_Jurisdictions

Steps to search for an entity

- User can search for an entity by providing
    - Partial name, full name or registration number of the entity
    - ISO country code of jurisdiction of incorporation of the entity

Note: The list of jurisdictions and corresponding ISO codes can be retrieved by using GET Jurisdictions

3.2 Create a case for an entity

API endpoint:

#	API endpoint	Method
1	Company case	#/Companies/post_v2_Companies
2	Jurisdictions	#/Jurisdictions/get_v2_Jurisdictions
3	Companies Search	#/Companies/post_v2_Companies_search
4	Company Types	#/CompanyTypes/get_v2_CompanyTypes

Prerequisite

User should determine if the jurisdiction of incorporation of the entity is automated in the KYC System. This information can be obtained from GET Jurisdictions endpoint

User should have the exact Entity name and registration number returned from the POST Companies Search endpoint.

Steps to create a case

a. Registered entity case automated jurisdiction

- User can create an entity case in an automated jurisdiction by providing
  - Entity name
  - Registration number
  - ISO country code of jurisdiction of incorporation of the entity
  - Case processing type - *By default, a Full KYC case will be created by the system, user can specify if they want to create an AML-only case.*

Important Note: The Entity name used in the request should be exactly the same as the entity name returned from the POST Companies Search endpoint. Where available, we recommend using the Registration number.

b. Entity case in non-automated jurisdictions

- User can create an entity case in a non-automated jurisdiction by providing
  - Entity name
  - ISO country code of jurisdiction of incorporation of the entity
  - Entity type
  - Case processing type - *By default a Full case will be created. User can specify if they want to check AML matches alone for the entity.*

Note: Entity type, ISO country code can be obtained from GET Company Types, GET Jurisdictions endpoints

c. Un-registered entity case in automated jurisdictions

API endpoint:

#	API endpoint	Method
1	Company types	#/CompanyTypes/get_v2_CompanyTypes
2	Jurisdictions	#/Jurisdictions/get_v2_Jurisdictions

- User can also create a case for an unregistered entity by providing:
    - Entity name
    - ISO country code of jurisdiction of incorporation of the entity
    - Entity type
    - Case processing type - *By default, a Full KYC case will be created. Users can specify if they want to check AML matches alone for the entity*

Note: Entity type, ISO country code can be obtained from Get Company Types, Get Jurisdictions endpoint.

d. Importing a case

API endpoint:

#	API endpoint	Method
1	Import company case	#/Companies/post_v2_Companies_import
2	Company Types	#/CompanyTypes/get_v2_CompanyTypes
3	Jurisdictions	#/Jurisdictions/get_v2_Jurisdictions
4	Company case properties	#/Companies/get_v2_Companies caseCommonId properties

- User can import an already prepared case into the KYC system using the Import Company Case endpoint by providing the following information. The cases imported are checked for AML matches only, full KYC case is not created for them
    - Entity name
    - ISO country code of jurisdiction of incorporation of the entity
    - Entity type- the company type
    - Case properties

Note: Entity type, ISO country code can be obtained from the GET Company Types, GET Jurisdictions endpoints. Existing case properties can be obtained from the GET Company Case Properties endpoint.

3.3 View case information

API endpoint:

#	API endpoint	Method
1	Companies	#/Companies/get_v2_Companies
2	Company details	#/Companies/get_v2_Companies caseCommonId_

Prerequisite

The case should already be present in the KYC system to use these endpoints.

Steps to view case information

User can obtain case information from Company details by providing *casecommonID*

How to obtain casecommon Id:

- *casecommonId* is returned when a case is created
- *casecommonId* can be obtained by browsing the case list using Companies,

Additional information

User can view a list of all available cases in their account or a single case in detail. View case endpoints present a birds-eye view of the case including basic case information. Details returned by these endpoints can be used to determine the answer for the following questions:

- What is the current status of the case? Whether the case is currently being worked on or closed
  - *status* - Acceptable values "Open" or "Closed";
- Whether the case has been built and is ready for review
  - *statusId* - represents the current state of the case. Available status identifiers can be found in Company details
- Was the case accepted or rejected?
  - *caseDecision*-final decision made for a closed case, either "Accepted" or "Denied"
- Is it an AML positive case?
  - *IsCaseAMLPositive* - Returns **True** if the case contains at least one AML check not excluded. **False** otherwise

3.3.1 Case properties

API endpoints:

#	API endpoint	Method
1	Company case properties	#/Companies/get_v2_Companies caseCommonId properties

Prerequisite

The case should be present in the KYC system to use this endpoint

Steps to view case information

- User can obtain additional case information from Get company case properties by providing *casecommonID*

Additional information

Additional information is added to specific cases to fulfil unique customer requirements. The Get company case properties endpoint is used to get additional case-specific information.

3.3.2 Entity Organisational chart

API endpoints:

#	API endpoint	Method
1	Organizational chart	#/Companies/get_v2_Companies caseCommonId org_chart

Prerequisite

The case should be present in the KYC system to use this endpoint.

Steps to view case information

- User can obtain a list of information required to build the entity's organizational chart from the Get organizational chart endpoint by providing *casecommonID*

3.4 View step information

API endpoints:

API endpoint:

#	API endpoint	Method
1	Case steps	#/CaseSteps/get_v2_CaseSteps caseCommonId_
2	Case step details	#/CaseSteps/get_v2_CaseSteps_caseCommonId__details__stepId_
3	Companies Case Step Activate	#/Companies/post_v2_Companies caseCommonId activate caseStepId_

Prerequisite

The case whose steps are being looked at should be present and ready in the KYC system to use these endpoints.

Steps to view step information

- A KYC case consists of multiple steps
- User can obtain the following information for each step in a case from Case steps by providing *casecommonID* of the case
  - *casestepID* - unique step id
  - *status* - Current status of the step (PASSED, FAILED, NOT REVIEWED)
- User can obtain details of a case step from Case step details by providing *casestepID* of the step

Additional information

- Case Steps response returns IsDeactivated as ‘true’ or ‘false’. It is ‘false’ for Officers and Shareholders of the case steps that require full KYC verification based on the AML and Sanctions lists screening. Where required a deactivated step can be activated for full KYC verification using Companies Case Step Activate endpoint

- Case step details return information based on the step type. Unique information is received for each step type.

We explore some unique step types and additional endpoints used to get information about these steps in the following subsections of this document.

3.4.1 Document step

API endpoints:

#	API endpoint	Method
1	Case step details	#/CaseSteps/get_v2_CaseSteps_caseCommonId__details__stepId_
2	Company documents	#/Companies/get_v2_Companies_caseCommonId__documents
3	List mandatory documents for company case	#/Companies/get_v2_Companies_caseCommonId _documents_rules_mandatory
4	Upload document to company case	#/Companies/post_v2_Companies_caseCommonId _documents_upload
5	Request company case documents	#/Companies/post_v2_Companies_caseCommonId _documents_request
6	Download document	#/Documents/get_v2_Documents_documentId_ document

Every entity case requires a list of mandatory documents to be attached to the case depending on the case jurisdiction. These documents are obtained by the KYC system from the registry or uploaded by the users. Additionally, some case-specific documents may be requested from end-users. To enable the user to accomplish these tasks, multiple endpoints are provided as discussed below.

- Case step details endpoint returns the following information for each document required to be attached to the step. This information can be obtained by providing *casestepID*
  - *Category* - The category of the document
  - *DocumentAvailable* - Indicates if document(s) is attached
  - *VerificationStatus* - Indicates whether the document was verified successfully
  - *CaseDocumentID* - unique identifier for the document
  - *Name* - Name of the document
  - *Link* - Link to document location for attached document

- Company documents endpoint returns all available documents currently attached to the case. This list can be obtained by providing *casecommonID*.

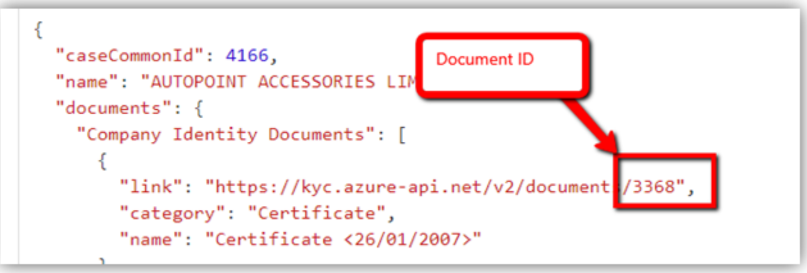
- List mandatory documents for company case endpoint returns a list of mandatory documents required to be attached to the case. This information is arrived at by using jurisdiction of incorporation of the case. This list can be obtained by providing *casecommonId*D

- Upload document to company case endpoint facilitates document upload to the case. To accomplish document upload *casecommonID* should be supplied along with the document to be uploaded. For mandatory documents file category should be supplied, this information can be obtained from List mandatory documents for company case endpoint.

- Request company case documents endpoint facilitates document request from end-user. To send a document request, *casecommonID* should be provided along with a list of documents to be requested. Email address or phone number of end-user should be provided to enable communication.

- Download document endpoint attached to the case. The document can be obtained by providing *documentID*

- *documentID* can be obtained from Company documents endpoint as shown in the image



```
{
  "caseCommonId": 4166,
  "name": "AUTOPOINT ACCESSORIES LIM
  "documents": {
    "Company Identity Documents": [
      {
        "link": "https://kyc.azure-api.net/v2/documents/3368",
        "category": "Certificate",
        "name": "Certificate <26/01/2007>"
      }
```

3.4.2 AML step

API endpoints:

#	API endpoint	Method
1	Case step details	#/CaseSteps/get_v2_CaseSteps caseCommonId details stepId_
2	Company AML Checks	#/Companies/get_v2_Companies_caseCommonId__amlchecks
3	Exclude AML step	#/CaseSteps/patch_v2_CaseSteps caseCommonId exclude stepId_

Each entity case created in the KYC system undergoes AML checks to flag potential matches.

- Case step details endpoint returns the following information for each potential AML match found for the case. This information can be obtained by providing *casestepID*
  - *category* - the type of AML entry
  - Detailed information about the match as obtained from AML data source

- Company AML Checks endpoint returns a list of all AML matches found for a case. This information can be obtained by providing *casecommonID.* The list contains following information about each potential match
  - *category* - the type of AML entry
  - Detailed information about the match as obtained from AML data source

- Exclude AML step facilitates the exclusion of an AML match result from further perusal. This is mostly used when a user feels that the match obtained may not be correct. This can be achieved by providing *casestepID* of the AML match to be excluded to Exclude AML step endpoint.

3.4.3 Linked companies/individuals

API endpoints:

#	API endpoint	Method
1	Case step details	#/CaseSteps/get_v2_CaseSteps caseCommonId details stepId_
2	Company members	#/Companies/get_v2_Companies_caseCommonId__members
3	Link case to company	#/Companies/post_v2_Companies_parentCaseCommonId_link_caseCommonId_

An entity has one or more companies/individuals associated with it as controlling bodies, shareholders or owners. For these associated companies/individuals, a separate case (sub-case) is created and linked to the original entity case via a step.

- Case step details endpoint returns following information for a step which is created for a linked case. This information can be obtained by providing *casestepID*
    - Identity information of subcase
    - Any additional unique case information (Case properties) of subcase
    - Information on how the subcase is related to the original entity case

- Company members endpoint returns a list of associated companies/individuals grouped by type of association. This information can be obtained by providing *casecommonID*.

- Link case to company endpoint facilitates linking of a subcase to the original entity case. This endpoint creates a new step in the original entity case with a link to the subcase. This can be achieved by providing:
    - *casecommonID* of the original entity case
    - *casecommonID* of the case to be linked
    - Type of association
    - Additional details based on type of association

3.5 Update case steps

API endpoints:

#	API endpoint	Method
1	Update step status	#/CaseSteps/patch_v2_CaseSteps caseCommonId status stepId_

Prerequisite

The case whose steps are being updated should already be present and ready in the KYC system to use these endpoints

Steps to update step

- User can mark each step of the case as pass or fail using Update step status by providing the following details. All steps will be in NOT REVIEWED status initially
  - *casestepID* - unique ID of the step to be updated
  - *status* -Step's new status (PASSED, FAILED, NOT REVIEWED)

3.6 Update case

3.6.1 Update case information

API endpoints:

#	API endpoint	Method
1	Update company case	#/Companies/put_v2_Companies caseCommonId identity
2	Create/Update company case properties	#/Companies/post_v2_Companies_caseCommonId__properties
3	Remove company case property	#/Companies/delete_v2_Companies_caseCommonId__properties__dataType_
4	Get data types	#/Companies/post_v2_Companies_caseCommonId__properties

Prerequisite
The case should be present in the KYC system to use these endpoints

Steps to update case

- User can update identity details of the case using the Update company case endpoint by providing:
  - *casecommonID of the case*
  - list of identity fields to be updated along with values

- User can update or create new case properties using the Create/Update company case properties endpoint by providing:
  - *Datatype* - User can opt to use existing datatypes or add new datatype on the go. Existing data types can be obtained by using Get data types endpoint. If datatype provided by the user is not on the list a new datatype will be created with the value supplied.
  - Value for the case property field

- User can remove case properties using the Remove company case property endpoint by providing:
  - *casecommonID* of the case
  - *Datatype* -Existing data types can be obtained by using Get data types endpoint

3.6.2 Update case status

API endpoint:

#	API endpoint	Method
1	Close/Reopen company case	#/Companies/patch_v2_Companies caseCommonId status

Prerequisite

The case should be present in the KYC system to use this endpoint.

Steps to update case status

- User can update the case status using Close/Reopen company case by providing the following details:
  - *caseCommonID* of the case to be updated
  - *status* -New status (Open or Close)

3.6.3 Delete case

API endpoint:

#	API endpoint	Method
1	Remove company case	#/Companies/delete_v2_Companies caseCommonId_

Prerequisite

The case should already be present in the KYC system to use this endpoint.

Steps to delete case

- User can delete a case using Remove company case by providing the *caseCommonID* of the case to be deleted.

3.7 Obtain case report

API endpoint:

#	API endpoint	Method
1	Download case report	#/Companies/get_v2_Companies caseCommonId report

Prerequisite

The case should already be present in the KYC system to use this endpoint.

Steps to obtain a closed case report

- User can obtain a case report for a case using the Download case report endpoint by providing *casecommonID* of the case.

3.8 Live Monitoring

3.8.1 Live Monitoring Alerts List

API endpoint:

#	API endpoint	Method
1	Live monitoring alerts list	#/Companies/post_v2_Companies_lm_cases

<u>Prerequisite</u>

The case should already be present in the KYC system to use this endpoint.

<u>Steps to get the list of cases which have active alerts along with the count of alerts</u>

- Case(s) details with active alerts can be obtained by sending a request via this API
- One or more of the following filters can be applied optionally for filtered results
    - caseCommonId
    - Filter by Case Assignee
    - Filter by Alert Type
    - AML alert types
    - Filter by Case Type
    - Filter by Root, Sub or All Cases
    - Filter by Open, Closed or All Cases
- If none of the filters are applied, then all the cases with alerts will be returned
- The endpoint returns the following
    - Name of the Case
    - Case Number
    - Address
    - Case Type (Entity/Individual)
    - Case Jurisdiction
    - Case Status (Live case/closed case)
    - Alert type:
        - Case Details Review alert count
        - Expired Documents alert count
        - Manual review alert count
        - AML alert count

3.8.2 Get Live Monitoring Alert Details

API endpoint:

#	API endpoint	Method
1	Live monitoring alert details	#/Companies/get_v2_Companies caseCommonId lm_alerts

Prerequisite

The case should already be present in the KYC system to use this endpoint.

Steps to get the live monitoring alert details for a case

- CaseCommonId is the mandatory parameter for this request
- Following are returned in the API response
  - Name of the Case
  - Case Number
  - Address
  - Case Type (Entity/Individual)
  - Case Jurisdiction
  - Case Status (Live case/closed case)
  - Case Step ID
  - Changes
    - The following section shall be displayed for each Review type alert of the case
      - Change id
      - Changes to Property
        - Property Name
        - New Value
      - Officer
        - Name
        - Address
        - Role
      - Shareholder
        - Name
        - Address
        - Shares held
      - New Document
        - Name of the document
      - Updated document
        - Name of the document
      - Removed Document
        - Name of the document

- AML alert
  - New/Updated AML Match
  - Name
  - AML match type
  - Country
  - Updated on (for Updated matches)
  - Biography (for new matches)

- Expiration alert
  - Expired document found/ POI is about to expire
  - Expiration in (number of days for POI is about to expire alert)
  - Document name
  - Expiration date

3.8.3 Action Live Monitoring Alert

API endpoint:

#	API endpoint	Method
1	Action live monitoring alert	#/Companies/post_v2_Companies caseCommonId lm_alerts_action

<u>Prerequisite</u>

- The case should already be present in the KYC system to use this endpoint.
- Have the Case ID and Alert ID that needs to be actioned. Step ID is Optional

<u>Steps to action live monitoring alert</u>

- To action an alert following parameters needs to be sent via the API mandatorily
  - Case ID
  - Alert ID
  - Action – The action that needs to be performed on the alert. The parameter supports the following values
    - Exclude
    - Apply
    - Dismiss
  - Step ID can optionally be provided in the API request
- Following table provides the highlights of system behaviour when a certain action is applied to an alert type

#	Action	Alert type	Action result
1	Exclude	Case details review	This action removes the alert from Live monitoring list and will not be applied to the case
2	Apply	Case details review	This action applies the alert to the case and removes it from the live monitoring list
3	Apply	Manual case review	This action opens the case for a manual review and the alert is removed from the live monitoring list
4	Apply	New/Updated AML match	When applied to a closed case ▪ This action adds or updates the AML matches for the case ▪ The alert is removed from live monitoring list ▪ The case is opened
5	Dismiss	New/Updated AML match	When applied to a live case ▪ The alert is removed from live monitoring list
6	Dismiss	POI expiration alert	This action removes the alert from live monitoring list

3.8.4 Set Review Date for a Case

API endpoint:

#	API endpoint	Method
1	Set review date for a case	#/Companies/put_v2_Companies caseCommonId review_date

Prerequisite

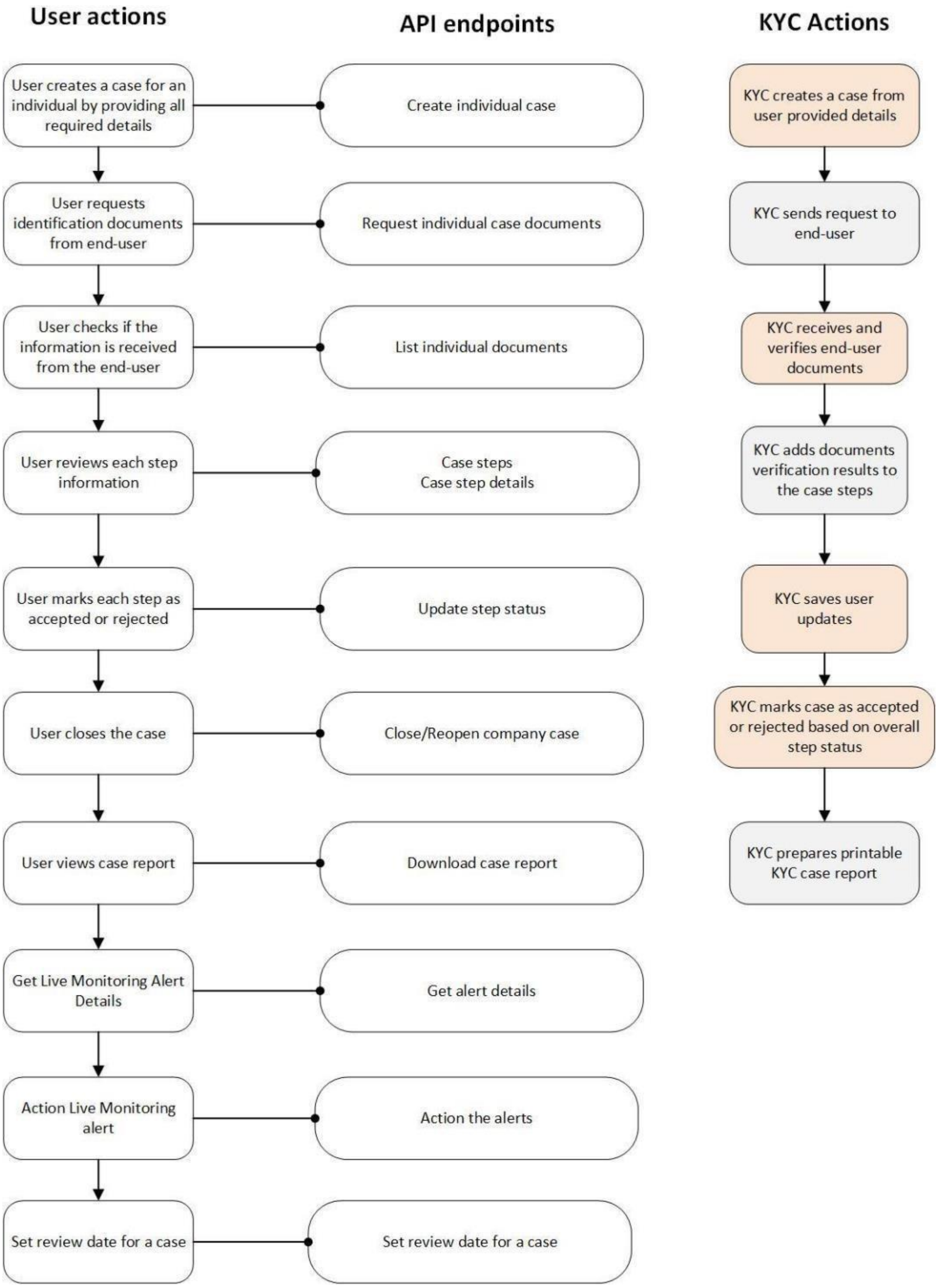
- The case should already be present in the KYC system to use this endpoint
- Have the case id of the case

Steps to set review date for a case

- The following parameters needs to be provided to the API to set a review date for a case
  - Case ID
  - Review Date – This can be any of the following options
    - Date in DD/MM/YYYY format
    - Do not review
    - Review now
    - 3 month
    - 6 month
    - 9 month
    - 1 year
    - 2 years
    - 3 years
    - 5 years
    - 10 years

4.0 Individual case

Please see below a usual flow of user interaction with Know Your Customer when preparing a compliance case for an individual.


User actions
API endpoints
KYC Actions
User creates a case for an individual by providing all required details
Create individual case
KYC creates a case from user provided details
User requests identification documents from end-user
Request individual case documents
KYC sends request to end-user
User checks if the information is received from the end-user
List individual documents
KYC receives and verifies end-user documents
User reviews each step information
Case steps
Case step details
KYC adds documents verification results to the case steps
User marks each step as accepted or rejected
Update step status
KYC saves user updates
User closes the case
Close/Reopen company case
KYC marks case as accepted or rejected based on overall step status
User views case report
Download case report
KYC prepares printable KYC case report
Get Live Monitoring Alert Details
Get alert details
Action Live Monitoring alert
Action the alerts
Set review date for a case
Set review date for a case

The next section provides a detailed breakdown of each step of a user's interaction with the Know Your Customer system for individual cases.

4.1 Create a case for an Individual

API endpoint:

#	API endpoint	Method
1	Create individual case	#/Individuals/post_v2_Individuals

Steps to create a case

- User can create an individual case by providing:
  - First name, Last name of individuals
  - Other details about the individual such as address, nationality and address

Import case

API endpoint:

#	API endpoint	Method
1	Import individual case	#/Individuals/post_v2_Individuals_import

Steps to import cases

- User can import already available case information into the KYC system using the Import individual case endpoint by providing the following information:
  - First name, Last name of individuals
  - Other details about the individual such as address, nationality and address

4.2 View case information

API endpoints:

#	API endpoint	Method
1	Individuals	#/Individuals/get_v2_Individuals
2	Individual Details	#/Individuals/get_v2_Individuals_caseCommonId_

Steps to view case information

Prerequisite

The case should be present in the KYC system to use these endpoints.

Steps to view case information

- A user can obtain case information from the Individual Details endpoint by providing *casecommonID*
    - *casecommonID* is returned when case is created
    - *casecommonID* can be obtained by browsing results obtained using the Individuals endpoint

4.2.1 Case properties

API endpoints:

#	API endpoint	Method
1	Individual case properties	#/Individuals/get_v2_Individuals caseCommonId properties

Prerequisite

The case should be present in the KYC system to use this endpoint.

Steps to view case information

- User can obtain additional case information from Get individual case properties by providing *casecommonID*

Additional information

Certain additional properties are added to the case to fulfil unique customer requirements. The Get individual case properties endpoint is used to get additional case-specific information.

4.3 Request document

API endpoints:

#	API endpoint	Method
1	Request individual case documents	#/Individuals/post_v2_Individuals caseCommonId documents_request
2	List mandatory documents for individual case	#/Individuals/get_v2_Individuals_caseCommonId__documents_mandatory

Steps to request document

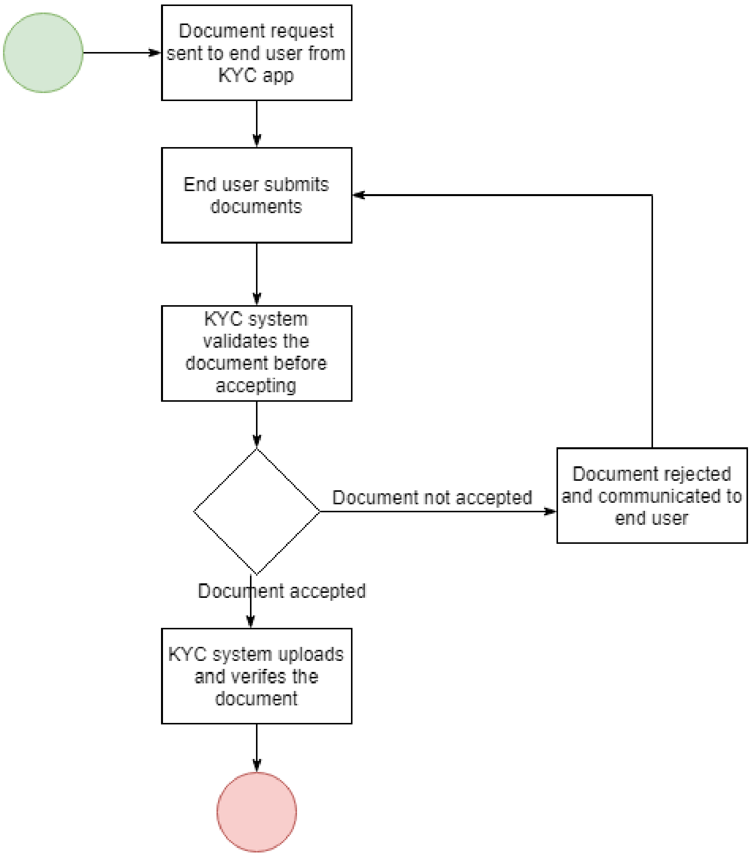
- User can request document from end-user by providing the following information:
  - *List of documents* to be requested from end-user
  - *Email* or *phone* number of end-user to send a document request

Note: List of mandatory documents for a case can be obtained from List mandatory documents for individual case by providing *casecommonID* of the case.

4.3.1 Pre-validating documents

API endpoint:

#	API endpoint	Method
1	Pre-validate document for individual case	#/Individuals/post_v2_Individuals_documents_prevalidate
2	List mandatory documents for individual case	#/Individuals/get_v2_Individuals_caseCommonId_documents_mandatory


Document request sent to end user from KYC app
End user submits documents
KYC system validates the document before accepting
Document not accepted
Document rejected and communicated to end user
Document accepted
KYC system uploads and verifes the document

- User can pre-validate documents uploaded by the end-user before accepting them for verification using Pre-validate document for individual case endpoint by providing:
  - *file category*
  - *name*
  - *Document submitted by end-user*

Note: Information on *file category, name* can be obtained from List mandatory documents for individual case endpoint by providing *casecommonID* of the case

4.3.2 Upload documents

API endpoint:

#	API endpoint	Method
1	Upload document to individual case	#/Individuals/post_v2_Individuals_caseCommonId__documents_upload
2	List mandatory documents for individual case	#/Individuals/get_v2_Individuals_caseCommonId__documents_mandatory

Steps to upload documents

- User can also upload documents to an individual case using Upload document to individual case by providing document and *casecommonID*:
  - *file category*
  - *name*
  - *Document of the end-user*

Note: Information on *file category, name* can be obtained from the List mandatory documents for individual case endpoint by providing *casecommonID* of the case.

Additional Information

When a document is uploaded using API, user can decide whether a new step should be created for the document or it is enough to add the document to the proof of identity step of the case. This can be achieved by using the *createNewStep* parameter of the endpoint.

4.4 View step information

API endpoint:

#	API endpoint	Method
1	Case steps	#/CaseSteps/get_v2_CaseSteps caseCommonId_
2	Case step details	#/CaseSteps/get_v2_CaseSteps_caseCommonId__details__stepId_

Prerequisite

The case whose steps are being looked at should be present and ready in the KYC system to use these endpoints.

Steps to view step information

- A KYC case consists of multiple steps
- User can obtain the following information for each step in a case from Case steps endpoint by providing *casecommonID* of the case
    - *casestepID* - unique step id
    - *status* - Current status of the step (PASSED, FAILED, NOT REVIEWED)
- User can obtain details of a case step using the Case step details endpoint by providing *casestepID* of the step

Additional information

The Case step details endpoint provides unique information based on the step type.
Some unique steps and additional endpoints used to get information about them are discussed in the following subsections.

4.4.1 Document step

API endpoints:

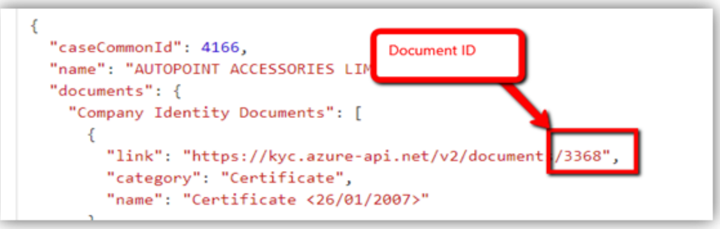
#	API endpoint	Method
1	Case step details	#/CaseSteps/get_v2_CaseSteps caseCommonId details stepId_
2	List individual documents	#/Individuals/get_v2_Individuals_caseCommonId__documents
3	Download case document	#/Documents/get_v2_Documents documentId_

- The Case step details endpoint returns the following information for each document/documents attached to the step. This information can be obtained by providing *casestepID*
    - *Category* - The category of the document
    - *DocumentAvailable* - Indicates if document(s) is available
    - *VerificationStatus* - Indicates whether the document was verified successfully
    - *CaseDocumentID* - Unique identifier for the document
    - *Name* - Name of the document
    - *Link* - Link to document location

- The List individual documents endpoint returns a list of documents attached to the individual case at the given time. This list can be obtained by using *casecommonID* of the case.

- The Download case document endpoint returns document attached to a case. The document can be obtained by providing *documentID*.

Note: *documentID* can be obtained from the List individual documents endpoint as shown in the image below:



```
{
  "caseCommonId": 4166,
  "name": "AUTOPOINT ACCESSORIES LIM
  "documents": {
    "Company Identity Documents": [
      {
        "link": "https://kyc.azure-api.net/v2/documents/3368",
        "category": "Certificate",
        "name": "Certificate <26/01/2007>"
```

4.4.2 AML step

API endpoints:

#	API endpoint	Method
1	Case step details	#/CaseSteps/get_v2_CaseSteps caseCommonId details stepId_
2	Get individual AML checks	#/Individuals/get_v2_Individuals_caseCommonId__amlchecks
3	Exclude AML step	#/CaseSteps/patch_v2_CaseSteps caseCommonId exclude stepId

Each Individual case created in KYC undergoes AML checks to flag potential matches

- The Case step details endpoint returns the following information for each potential AML match found for the case. This information can be obtained by providing *casestepID*
  - *category* - the type of AML entry
  - Detailed information about the match as obtained from AML data source

- The Get individual AML checks step endpoint returns the following information for all AML matches found for a case. This information can be obtained by providing *casecommonID*
  - *category* - the type of AML entry
  - Detailed information about the match as obtained from AML data source

- The Exclude AML step endpoint facilitates the exclusion of an AML match result from further perusal. This is mostly used when a user feels that the match obtained may not be correct. This can be achieved by providing *casestepID* of the AML match to be excluded to Exclude AML step endpoint.

4.4.3 Linking Companies/Individuals

An individual can be linked to another individual or a company he/she has some relationship to.

#	API endpoint	Method
1	Link case to company	#/Individuals/post_v2_Individuals parentCaseCommonId link caseCommonId_

Link case to company endpoint facilitates linking of individual/entity case to the original individual case. This can be achieved by providing

- *casecommonID* of the original entity case
- *casecommonID* of the case to be linked
- Type of association - A list can be found in Link case to company page
- Additional details based on type of association

Separate steps are not created in an individual case when Companies/Individuals are linked. Linked companies/Individuals are listed under the associated company/associated individual step of the original case.

4.5 Update case step

API endpoints:

#	API endpoint	Method
1	Update step status	#/CaseSteps/patch_v2_CaseSteps caseCommonId status stepId_

Prerequisite

The case whose steps are being updated should be present and ready in the KYC system to use this endpoint.

Steps to update step

- User can mark each step of the case as pass or fail using Update step status by providing the following details. All steps will be in NOT REVIEWED status initially
  - *casestepID* - unique ID of the step to be updated
  - *status* - Step's new status (PASSED, FAILED, NOT REVIEWED)

4.6 Update case

4.6.1 Update case information

API endpoints:

#	API endpoint	Method
1	Update individual case	#/Individuals/put_v2_Individuals caseCommonId identity
2	Create/Update individual case properties	#/Individuals/post_v2_Individuals__caseCommonId_properties
3	Remove individual case property	#/Individuals/delete_v2_Individuals_caseCommonId__properties__dataType_
4	Get data types	#/Individuals/post_v2_Individuals caseCommonId properties

Prerequisite

The case should already be present in the KYC system to use these endpoints.

Steps to update case

- User can update identity details of the case using Update individual case identity by providing
  - *casecommonID of the case*
  - list of identity fields to be updated along with values
- User can update or create new case properties for a case using Create/Update individual case properties , by providing:
  - Datatype - User can opt to use existing datatypes or add new datatypes on the go. Existing data types can be obtained by using the Get data types endpoint. If datatype provided by the user is not on the list a new datatype will be created with the value supplied
  - Value for the case property field
- User can remove case properties using the Remove individual case property endpoint by providing
  - *casecommonID* of the case
  - *Datatype* -Existing data types can be obtained by using Get data types endpoint.

4.6.2 Update case status

API endpoint:

#	API endpoint	Method
1	Close/Reopen individual case	#/Individuals/patch_v2_Individuals caseCommonId status

Prerequisite

The case should be present in the KYC system to use this endpoint.

Steps to update case status

- User can update the case status using Close/Reopen individual case by providing the following details;
    - *caseCommonID* of the case to be updated
    - *status* -New case status (Open or Close)

4.6.3 Delete case

API endpoint:

#	API endpoint	Method
1	Remove individual case	#/Individuals/delete_v2_Individuals caseCommonId_

Prerequisite

The case should be present in the KYC system to use this endpoint.

Steps to delete case

- User can delete a case status using Remove individual case by providing the *caseCommonID* of the case to be deleted

4.7 Obtain close case report

API endpoint:

#	API endpoint	Method
1	Download individual report	#/Individuals/get_v2_Individuals caseCommonId report

Prerequisite

The case should already be present in the KYC system to use this endpoint.

Steps to obtain a closed case report

- User can obtain a case report file for a case using the Download individual report endpoint by providing *casecommonID* of the case.

4.8 Live Monitoring

4.8.1 Live Monitoring Alerts List

API endpoint:

#	API endpoint	Method
1	Live monitoring alerts list	#/Individuals/post_v2_Individuals_lm_cases

Prerequisite
The case should already be present in the KYC system to use this endpoint.

Steps to get the list of cases which have active alerts along with the count of alerts

- Case(s) details with active alerts can be obtained by sending a request via this API
- One or more of the following filters can be applied optionally for filtered results
  - caseCommonId
  - Filter by Case Assignee
  - Filter by Alert Type
  - AML alert types
  - Filter by Case Type
  - Filter by Root, Sub or All Cases
  - Filter by Open, Closed or All Cases
- If none of the filters are applied, then all the cases with alerts will be returned
- The endpoint returns the following
  - Name of the Case
  - Case Number
  - Address
  - Case Type (Entity/Individual)
  - Case Jurisdiction
  - Case Status (Live case/closed case)
  - Alert type:
    - Case Details Review alert count
    - Expired Documents alert count
    - Manual review alert count
    - AML alert count

4.8.2 Get Live Monitoring Alert Details

API endpoint:

#	API endpoint	Method
1	Live monitoring alert details	#/Individuals/get_v2_Individuals caseCommonId lm_alerts

<u>Prerequisite</u>

The case should already be present in the KYC system to use this endpoint.

<u>Steps to get the live monitoring alert details for a case</u>

- CaseCommonId is the mandatory parameter for this request
- Following are returned in the API response
    - Name of the Case
    - Case Number
    - Address
    - Case Type (Entity/Individual)
    - Case Jurisdiction
    - Case Status (Live case/closed case)
    - Case Step ID
    - Changes
        - The following section shall be displayed for each Review type alert of the case
            - Change id
            - Changes to Property
                - Property Name
                - New Value
            - Officer
                - Name
                - Address
                - Role
            - Shareholder
                - Name
                - Address
                - Shares held
            - New Document
                - Name of the document
            - Updated document
                - Name of the document
            - Removed Document
                - Name of the document
            - AML alert
                - New/Updated AML Match
                - Name
                - AML match type
                - Country
                - Updated on (for Updated matches)
                - Biography (for new matches)

- Expiration alert
  - Expired document found/ POI is about to expire
  - Expiration in (number of days for POI is about to expire alert)
  - Document name
  - Expiration date

4.8.3 Action Live Monitoring alert

API endpoint:

#	API endpoint	Method
1	Action live monitoring alert	#/Individuals/post_v2_Individuals caseCommonId lm_alerts_action

Prerequisite

- The case should already be present in the KYC system to use this endpoint.
- Have the Case ID and Alert ID that needs to be actioned. Step ID is Optional

Steps to action live monitoring alert

- To action an alert following parameters needs to be sent via the API mandatorily
  - Case ID
  - Alert ID
  - Action – The action that needs to be performed on the alert. The parameter supports the following values
    - Exclude
    - Apply
    - Dismiss
  - Step ID can optionally be provided in the API request
- Following table provides the highlights of system behaviour when a certain action is applied to an alert type

#	Action	Alert type	Action result
1	Exclude	Case details review	This action removes the alert from Live monitoring list and will not be applied to the case
2	Apply	Case details review	This action applies the alert to the case and removes it from the live monitoring list
3	Apply	Manual case review	This action opens the case for a manual review and the alert is removed from the live monitoring list
4	Apply	New/Updated AML match	When applied to a closed case ▪ This action adds or updates the AML matches for the case ▪ The alert is removed from live monitoring list ▪ The case is opened
5	Dismiss	New/Updated AML match	When applied to a live case ▪ The alert is removed from live monitoring list
6	Dismiss	POI expiration alert	This action removes the alert from live monitoring list

4.8.4 Set Review Date for a Case

API endpoint:

#	API endpoint	Method
1	Set review date for a case	#/Individuals/put_v2_Individuals caseCommonId review_date

<u>Prerequisite</u>

- The case should already be present in the KYC system to use this endpoint
- Have the case id of the case

<u>Steps to set review date for a case</u>

- The following parameters needs to be provided to the API to set a review date for a case
  - Case ID
  - Review Date – This can be any of the following options
    - Date in DD/MM/YYYY format
    - Do not review
    - Review now
    - 3 month
    - 6 month
    - 9 month
    - 1 year
    - 2 years
    - 3 years
    - 5 years
    - 10 years

5.0 Working with the case

5.1 Assign case to a user

API endpoint:

#	API endpoint	Method
1	Assign User to Case	#/AssignUser/put_v2_AssignUser caseCommonId assign userId_
2	Users	#/User/post_v2_User_list

Prerequisite

The case and users should be present in the KYC system to use this endpoint.

Steps to assign the case to a user

- User can assign a case to a user by providing the following information to the Assign User to Case endpoint
- *casecommonID* of the case to be assigned
- *userID* of the user to whom the case has to be assigned

Note: *userID* can be obtained using the Users endpoint

5.2 Use step note feature

API endpoints:

#	API endpoint	Method
1	Case step notes	#/CaseStepNotes/get_v2_CaseStepNotes caseCommonId stepId_
2	Add case step note	#/CaseStepNotes/post_v2_CaseStepNotes_caseCommonId____stepId_
3	Delete case step notes	#/CaseStepNotes/delete_v2_CaseStepNotes_caseCommonId____stepId___stepNoteId_

Prerequisite

The case should be present in the KYC system to use this endpoint.

Steps to use step notes feature

- User can obtain list of notes added to a step using the Case step notes endpoint by providing *casecommonID* of the case to which the step belongs and *casestepID* of the step itself
- User can add step notes using the Add case step note endpoint by providing *casecommonID* of the case to which the step belongs and *casestepID* of the step itself
- User can delete step notes using the Delete case step notes endpoint by providing *casecommonID* of the case to which the step belongs, *casestepID* of the step and *noteIDs* of notes to be deleted. *noteIDs* can be obtained from the Case step notes endpoint

5.3 View audit trail of a case

API endpoints:

#	API endpoint	Method
1	Company audit trail	#/Companies/get_v2_Companies caseCommonId audittrail
2	Individual audit trail	#/Individuals/get_v2_Individuals_caseCommonId__audittrail

Prerequisite

The case should be present in the KYC system to use this endpoint.

Steps to get the audit trail of a case

- User can find out what actions were taken on the case, by which user and when using audit trail endpoints by providing *casecommonID of* the case for which the audit trail needs to be obtained.

6.0 API Error Codes

HTTP Code	Description	Message Body

400	Bad Request	{
		"statusCode": 400,
		"message": "string",
		"apiErrors": [
		{
		"description": "string",
		"timeStamp": "string"
		}
		]
		}

404	Not found error	{
		"statusCode": 404,
		"message": "string",
		"apiErrors": [
		{
		"description": "string",
		"timeStamp": "string"
		}
		]
		}

500	Unexpected Error	{
		"statusCode": 500,
		"message": "Api Error",
		"apiErrors": [
		{
		"description": "Internal Error",
		"timeStamp": "dd/mm/yyyy hh:mm:ss"
		}
		]
		}

504	Gateway Timeout Error	No body returned **Notes:** 1. The search times for each jurisdiction vary from less than 5 seconds to up to 150 seconds. 2. From technical point of view, if the search is implemented with API, it should be very quick but if implemented with browser service then it is expected to be slow. 3. The maximum gateway timeout in K8S cluster is set to 300 seconds.

Know Your Customer Limited

Spaces, 8 Queen Street East,
Wan Chai, Hong Kong

https://knowyourcustomer.com