



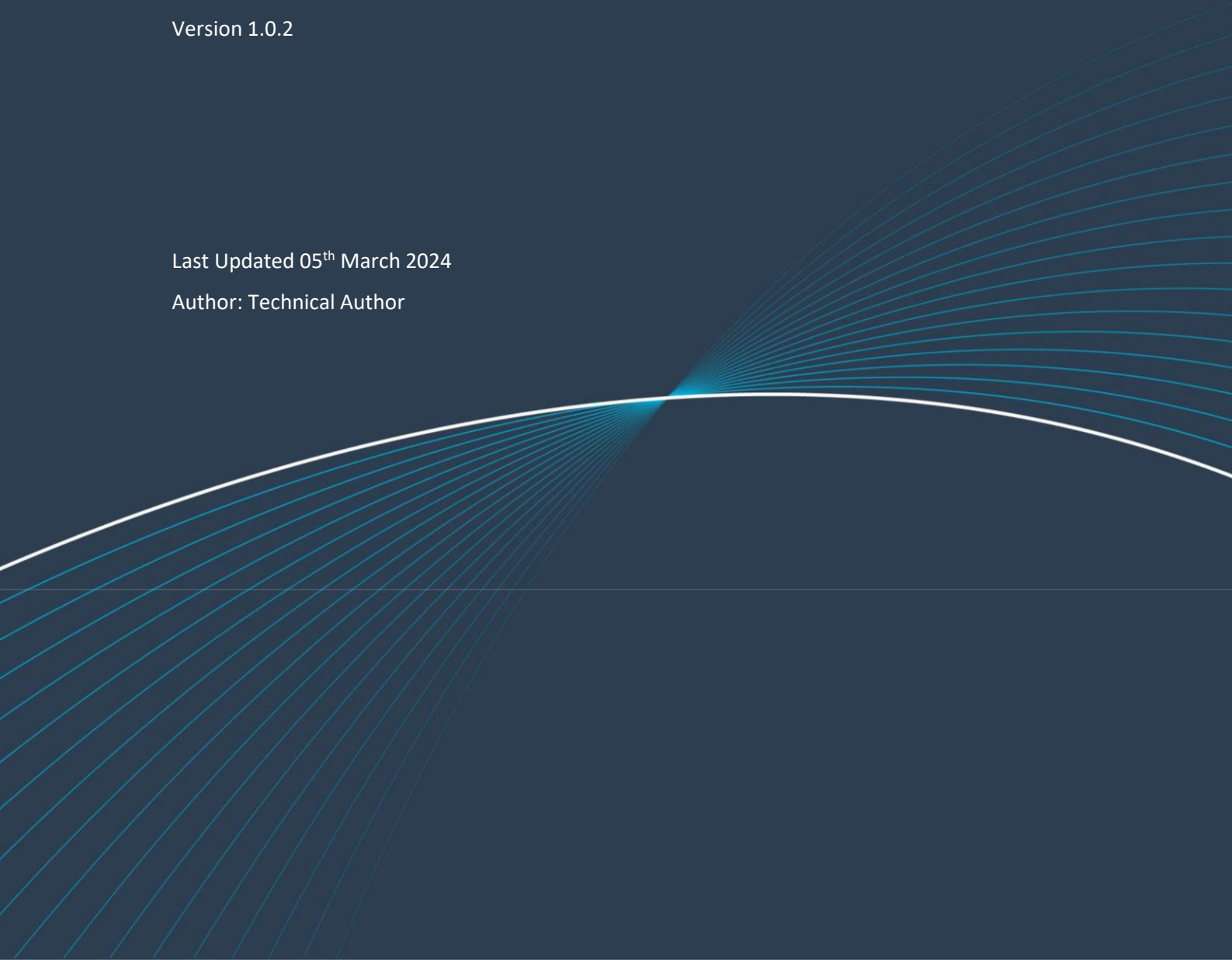
KYC Protect

Basic API Integration Guide

Version 1.0.2

Last Updated 05th March 2024

Author: Technical Author



Contents

Introduction	5
Integration Process Overview	7
Authentication	8
Introduction.....	8
Endpoint	8
Process Overview	8
Handling Responses.....	8
Best Practices.....	9
Create A Profile	10
Introduction.....	10
Endpoint	10
Best Practices for Naming Profiles.....	10
Required Properties for Profile Creation	10
Example Usage.....	11
Additional Information	11
Update Profile Details	12
Introduction.....	12
Endpoint	13
Best Practices for managing Details	13
Required Parameters and Properties for Updating Profile Details.....	13
Example Usage.....	14
Additional Information	14
AML Screening - Individual Searches	15
Introduction.....	15
Search For An Individual	16
Introduction.....	16
Endpoint	17
Best Practice for conducting AML Search.....	18
Required Parameters and properties for conducting AML Search.....	19
Return Individual Search Hits	20
Introduction.....	20
Endpoint	22
Update Search Hits	23
Introduction.....	23
Single Hit Update.....	24
Batch Update	25
Return Full Search Hit Information	26
Introduction.....	26
Endpoint	27
Required Parameters.....	27

AML Screening - Business Searches	28
Introduction.....	28
Search For A Business	30
Introduction.....	30
Endpoint	31
Required Parameters.....	31
Return Business Search Hits	33
Introduction.....	33
Endpoint	35
Update Search Hits	36
Introduction.....	36
Single Hit Update.....	37
Batch Update	38
Return Full Search Hit Information	39
Introduction.....	39
Endpoint	39
Required Parameters.....	39
Adding A Search to a Profile	40
Introduction.....	40
Endpoint	41
Required Parameters:.....	41
Example Usage.....	42
Batch Addition	42
Adding Search To Monitoring	43
Introduction.....	43
Endpoint	44
Required Properties.....	44
Additional Information	45
Update Monitoring Schedules	46
Introduction.....	46
Update Multiple Schedules	47
Endpoint	47
RequestBody Requirements	47
Example	48
Update a Single Schedule	49
Endpoint	49
Required Properties.....	49
Example	50
Appendices	51
Appendix A	51
Additional Endpoints Post Profile Creation	51
Appendix B.....	52
Additional Endpoints at Profile Detail Level	52

Appendix C.....	53
Additional Endpoints post Individual / Business Search	53
Appendix D	54
Additional Endpoints at Search Hits Level	54
Appendix E.....	55
Individual and Business Dataset Tables	55

Introduction

Welcome to the basic guide for integrating KYC Protect into your systems. This guide is crafted to ensure you can leverage the full potential of KYC Protect with ease and efficiency. Starting with the fundamental steps for integration, we will guide you through the advanced features, ensuring a robust setup for your KYC processes.

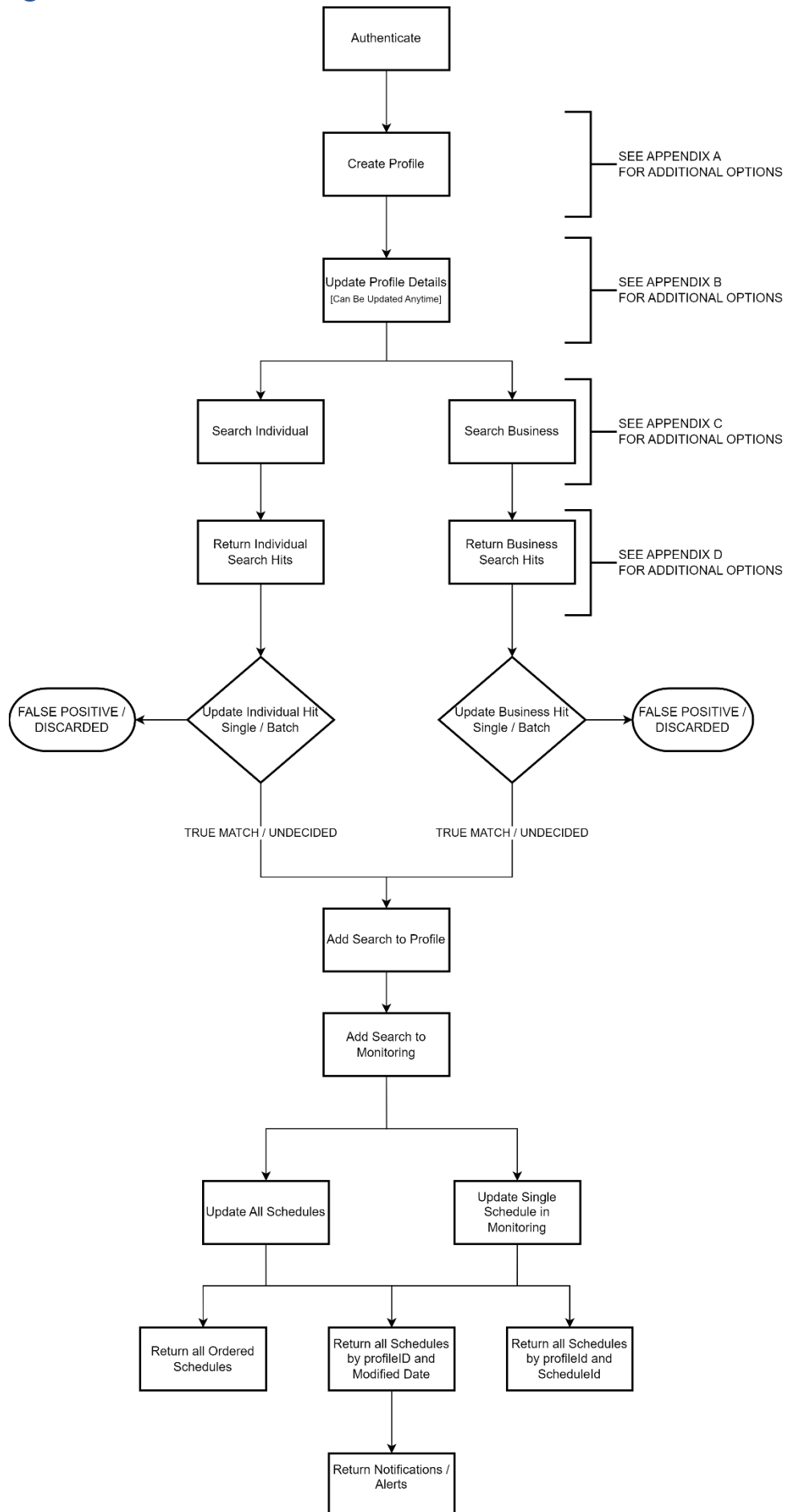
Within this guide, you will find a systematic approach to utilizing KYC Protect, emphasizing the following critical aspects:

1. **Process Flow:** A step-by-step walkthrough of the essential endpoints necessary for initializing your KYC verification process. This section aims to provide a roadmap for starting your KYC checks with confidence.
2. **Endpoint Details:** Detailed explanations of each endpoint, designed to give you comprehensive insights into their functions and how they can be used to meet your KYC requirements.
3. **Profile Setup:** Guidance on setting up profiles within KYC Protect, including essential configurations to ensure accurate KYC checks.
4. **Performing Screening:** Instructions on how to conduct thorough screenings using KYC Protect, including tips for optimizing your screening processes to yield accurate results.
5. **Setting Up Monitoring:** An overview of how to set up continuous monitoring for ongoing KYC compliance, ensuring that any changes in your customer's status are promptly identified and managed.
6. **Adjusting Screening and Monitoring Parameters:** A look into how to fine-tune your screening and monitoring settings, allowing for a customized approach that aligns with your specific risk management strategies.
7. **Handling Notifications and Alerts:** Insights into managing notifications and alerts generated by KYC Protect, enabling you to respond swiftly to any potential issues or changes in KYC status.

By following this guide, you will be equipped to integrate and utilize KYC Protect effectively, ensuring your projects benefit from enhanced compliance and security. Whether you are new to KYC Protect or looking to deepen your understanding of its capabilities, this guide aims to provide you with the knowledge and tools needed for successful integration.

NOTE: We highly recommend using the integration document available at: [Creditsafe Connect API Documentation - Creditsafe](#) for reference, which complements this help guide by providing additional insights into request parameters and responses.

Integration Process Overview



Authentication

Introduction

Initiating a secure connection with our API begins with the authentication process. Successful authentication grants you a unique 'Token', pivotal for subsequent interactions with the API.

Key Aspects of Authentication:

- **Token Usage:** This token is indispensable for establishing a secure link to the server. It is a prerequisite for the 'Header of every HTTP request made thereafter, ensuring that each request is securely associated with your authenticated session.

Endpoint

Method: POST

URL: <https://connect.creditsafe.com/v1/authenticate>

Process Overview

- **Submit Authentication Request:** Initiate the authentication by sending a POST request to the endpoint provided.
- **Token Retrieval:** Upon receiving a response, extract the 'Token from the payload. This token is your key to accessing the API's functionalities.
- **Token Inclusion in Subsequent Requests:** Embed the obtained token in the 'Header of all your HTTP requests. This step is crucial for maintaining a secure and authenticated session.

Handling Responses

- **Successful Authentication:** You will receive a token in the response, which you must include in the header of subsequent API calls.
- **Error Response 401 - Invalid Token:** Indicates either an expired or invalid token. Tokens have a validity period of 1 hour. If you encounter this error, re-authenticate to acquire a new token, ensuring uninterrupted access to the API.

Best Practices

- **Token Expiry Management:** Be mindful of the token's one-hour validity. Implement checks in your application to handle re-authentication smoothly, avoiding service disruption.
- **Secure Token Handling:** Treat the token as sensitive information. Ensure secure storage and transmission to protect your API access.

By adhering to these guidelines, you ensure a secure and effective use of the API, leveraging the full spectrum of features offered by our platform.

Create A Profile

Introduction

Creating a profile is an essential initial step in organizing your compliance checks within the Creditsafe system. Profiles act as containers for searches, attachments, notes, addresses, and key parties related to a specific entity.

Endpoint

Tag: KYC Profile Management

Method: POST

URL: <https://connect.creditsafe.com/v1/compliance/kyc-protect/profiles>

This endpoint is used to create a new profile in the system.

Best Practices for Naming Profiles

- **Reflective Naming:** Choose a profile name that reflects the entity being checked to facilitate easy identification. Although any string can be used, a name that clearly corresponds to the search entity is recommended.
- **Uniqueness:** Each profile name must be unique within the system to prevent confusion and ensure accurate identification.

Required Properties for Profile Creation

To create a profile, the following parameters are necessary:

- **Name:** The unique identifier for the profile.
- **Type:** The type of entity the profile represents. This parameter accepts ENUM values like trust, individual, soletrader, company, plc, partnership, otherEntity.
- **Details:** A nested object containing further attributes of the profile, such as:
 - **legalName:** The official legal name of the entity (required).

Example Usage

If conducting a search on "Creditsafe," you should create a profile named "Creditsafe." This profile will consolidate all relevant searches, notes, and documents. For different entities, establish separate profiles with unique names to organize related data effectively.

Request Body Example:

```
{
  "name": "string",
  "type": "trust",
  "details": {
    "legalName": "string",
  }
}
```

Note:

If the profile name is already in use you will receive an error response.

Please refer to the integration documentation for the Error Responses.

Additional Information

- **On Creation:** You can include other known details at the time of profile creation, not just the mandatory parameters.
- **Post-Creation Updates:** Profiles can be updated after creation to add or amend details, ensuring they remain comprehensive and up-to-date.

For more detailed information on integrating with our API and utilising this endpoint, please visit our [documentation](#).

Update Profile Details

Introduction

Enhancing the details of a profile is a pivotal process, allowing you to enrich the profile with comprehensive high-level information that characterises the entity. The details section is the core where vital information about the created profile is stored.

Important Aspects to Consider:

- **Validation Checks:** This endpoint is designed with validation mechanisms to ensure data integrity and relevance. Providing information not pertinent to the selected profile type will trigger an error, clearly outlining the nature of the discrepancy.

Example: Inputting an 'organizationNumber' for profiles designated as 'Individual' or 'SoleTrader' will lead to a validation error, indicating the provided data's incompatibility with the profile type.

- **Consultation with Integration Document:** To fully understand where validations occur and ensure compliance with them, it is essential to consult the [integration document](#). This document details the properties in the request body subject to validation and outlines allowable selections based on the profile type. This guidance is crucial for avoiding validation errors and making informed updates.
- **Flexibility of Updates:** You have the liberty to update the profile details at any stage. However, it is particularly recommended as a subsequent step post-profile creation to supplement the profile with additional detailed information as it becomes available.
- **Mandatory Field:** The 'legalName' is a requisite in every update operation. Typically, this field remains constant once set, especially in the context of individual profiles.

Endpoint

This functionality is accessible under the KYC Individual Profile Management tag within our online integration documentation, providing a structured pathway for easy reference.

Tag: [KYC Individual Profile Management](#)

Method: PUT

URL: <https://connect.creditsafe.com/v1/compliance/kyc-protect/profiles/{profileId}/details>

Best Practices for managing Details

- **Data Validation:** Ensure that provided details are compatible with the profile type to avoid validation errors.
- **Legal Name Requirement:** 'legalName' is mandatory for every update and must be consistent.
- **Continuous Update:** Profile details can be updated at any stage to incorporate new or revised information.

Required Parameters and Properties for Updating Profile Details

To update profile details, the following parameters and properties are necessary:

Path Parameter: {profileId}

This item is acquired from the 'Create Profile' Response

RequestBody Properties:

- **Details:** A nested object containing further attributes of the profile, such as:
 - **legalName:** The official legal name of the entity (required).

Example Usage

```
{
  "legalName":      "Creditsafe Ltd",
  "activity":       "62409",
  "description":    "Example Free Text",
  "email":          "example@creditsafe.com",
  "website":        "www.creditsafe.com",
  "organizationNumber": "12345678",
  "vatNo":          "GB12345678",
}
```

The example above demonstrates how to update the 'details of a profile. This update introduces new information to the details section after the initial creation of the profile named 'Creditsafe'.

The 'legalName of 'Creditsafe Ltd is included again to show that while it remains unchanged, additional data can be appended to enhance the profile's richness.

Additional Information

Note: The 'legalName field, being a required field, is resubmitted to maintain consistency, even without changes. It is pivotal to ensure that all other information provided, such as 'organizationNumber or 'vatNo', adheres to the validation criteria as outlined in our integration documentation. This diligence helps in avoiding validation errors and ensures a smooth update process.

Operational Insights:

Utilise this endpoint to refine profiles, ensuring they accurately depict the entity's attributes. By following the validation rules and updating information as needed, you maintain the accuracy and relevance of your compliance profiles.

AML Screening - Individual Searches

Introduction

AML Screening for individuals is a critical component of our compliance toolkit, designed to thoroughly vet individuals through a structured and comprehensive search process. This process is divided into three primary sections and includes an additional optional endpoint for enhanced scrutiny.

Core Sections of Individual AML Screening:

- **Perform the Search for an Individual:** Initiate a detailed search to identify potential matches or risks associated with an individual. [\[Detailed Description HERE\]](#)
- **Return the Search Hits for the Search:** After conducting the search, review the hits or matches found to further analyse and determine their relevance. [\[Detailed Description HERE\]](#)
- **Update the Hits to Determine Status:** Each hit requires evaluation to classify the nature of the match. The outcomes include: [\[Detailed Description Here\]](#)
 - **True Match:** Confirming the hit is accurately identified with the individual.
 - **False Positive:** Determining the hit is incorrectly associated with the individual.
 - **Undecided:** Cases where a definitive conclusion cannot be reached.
 - **Discarded:** Hits that are deemed irrelevant or incorrect and are thus disregarded.

Note: These can either be updated in batch or individually.

Optional Endpoint:

- **Return Full Details on a Specific Search Hit:** For hits that require deeper investigation, this optional endpoint allows for retrieving comprehensive details about a specific match. [\[Detailed Description HERE\]](#)

Search For An Individual

Introduction

Conducting an Individual search within KYC AML Screening framework is streamlined to ensure precise and relevant results. To initiate a search, a combination of parameters must be provided:

One of the following options should be utilized, not both:

- firstName
- middleName
- lastName
- threshold (Required)
- datasets (Required)

OR

- name
- threshold (Required)
- datasets (Required)

Greater accuracy of a search hit can be achieved if the first option is utilised for an Individual search.

Endpoint

Endpoint Usage:

This operation is categorized under the KYC AML Screening – Individuals tag in our online integration documentation for easy reference.

Tag: [KYC AML Screening – Individuals](#)

Method: POST

URL: <https://connect.creditsafe.com/v1/compliance/kyc-protect/searches/individuals>

Example Request Body:

```
{
  "countryCodes": [
    "string"
  ],
  "threshold": 80,
  "firstName": "donald",
  "middleName": "john",
  "lastName": "trump",
  "gender": "male",
  "dateOfBirth": "1946-06-19",
  "pepTiers": "",
  "datasets": [
    "PEP", "SAN"
  ]
}
```

The 'Tag in our online documentation serves as a navigational aid, guiding you to the relevant section for detailed information about using this specific endpoint.

Best Practice for conducting AML Search

1. Profile Naming Importance:

- Accurate and meaningful naming of profiles is crucial in the AML Screening process.

2. Searches and Profiles:

- Searches can be conducted independently, but their full value is realized when linked to profiles.

3. Monitoring and Linkage:

- Monitoring capabilities require linking searches to the correct profile, ensuring that outcomes are properly associated.

4. Enhanced Workflow:

- Linking searches to profiles streamlines the compliance and verification workflow, making the search results more relevant.

5. Utilizing AML Screening Features:

- To fully utilize AML Screening functionalities, including continuous monitoring, searches must be linked to profiles.

Required Parameters and properties for conducting AML Search

Threshold: An integer value that sets the minimum confidence score for search results. Valid options include: 75, 80, 85, 90, 95, 100. Only search results that meet or exceed this threshold will be returned, allowing you to filter results based on their relevance and accuracy.

Datasets: Specifies the type of data you wish to include in your search. Depending on the nature of your compliance checks, you may require information from one or more of the following datasets:

- AM - Adverse Media
- DD - Disqualified Director
- NS - Insolvency
- PEP - Politically Exposed Persons (All)
- PEP-CURRENT` - Only Current PEPS
- PEP-FORMER` - Only Former PEPS
- PEP-LINKED` - Only linked PEPs (PEP by Association)
- POI - Profile of Interest
- ENF - Enforcement
- SAN - Sanctioned (All)
- SAN-CURRENT - Only current Sanctions
- SAN-FORMER - Only former Sanctions

To include multiple datasets in your search, list the three-letter codes in an array within the request body.

By adhering to these guidelines and utilizing the specified parameters, you can effectively perform targeted business searches that align with your compliance and risk management objectives.

The response will provide details of the search and a number of undecided hits associated to that search. It is at this point the next endpoint needs to be called to differentiate between those hits to determine the success of the search.

The property 'id' in the response to this endpoint is what will represent the 'searchID for future interaction. This id will be important for any future dealings with this search and any further actions.

Return Individual Search Hits

Introduction

Following the initiation of an individual search, retrieving the detailed outcomes is facilitated through the endpoint detailed below, which necessitates the inclusion of the 'searchId' from the initial search summary.

Understanding the Results:

- **Result Presentation:** Results yielding more than one potential match are displayed in an array, each with a 'hitScore' to quantify the match's relevance.
- **Identification of Hits:** Within this response, each item contains a unique 'hitId', crucial for the next step of evaluating and updating the relevance of each hit. This 'hitId', along with the 'searchId', plays a vital role in accurately categorizing the search outcomes.
- **Categorising Search Hits:** Each hit must be evaluated and categorized based on its relevance:
 - **True Match:** Accurately identifies the individual sought.
 - **False Positive:** Incorrectly associates the hit with the individual.
 - **Undecided:** Ambiguity regarding the hit's relevance.
 - **Discarded:** The hit is irrelevant and excluded.

The information provided in the summary should facilitate an informed decision on the individual's relevancy of interest.

Important Consideration:

If the evaluation of a hit leans towards "Undecided" or "True Match," it is advisable to link this information to the respective profile after updating the status.

This linkage is part of the process flow, ensuring that potentially relevant or confirmed individuals are accurately documented within their profiles.

The clear differentiation between the 'searchId' and the 'hitId' will become crucial in later stages, underscoring the need for meticulous attention to these identifiers during the update process.

Note: Summary information is not stored in the database at this juncture, serving solely for decision-making purposes.

Proceeding with Hit Updates: To accurately reflect the relevance of search hits, the designated endpoint for their evaluation and status update is required.

Endpoint

Listed under KYC AML Screening – Individuals in our online integration documentation for straightforward reference:

Tag: [KYC AML Screening - Individuals](#)

Method: GET

URL:

<https://connect.creditsafe.com/v1/compliance/kyc-protect/searches/individuals/{searchId}/hits>

By utilizing this endpoint, you can thoroughly review individual search hits, making informed decisions about their relevance and effectively updating their status.

This step is critical in refining search results and ensuring actions are based on accurate and relevant data, with the subsequent potential linkage to profiles enhancing the overall integrity and utility of the compliance checks.

Update Search Hits

Introduction

There are two methods to update search hits, in the event that only one search hit needs to be updated there is an endpoint that will specifically deal with a single case.

In the event that more than once hit is returned the 'batch update' can be used. Since all hits needs to be dealt with, it is most likely that this endpoint will be used.

Single Hit Update

Updating the status of a single search hit is essential, as each hit identified during the AML Screening process necessitates a definitive action. This operation allows you to accurately categorize the relevance or accuracy of an individual hit.

Endpoint

Tag: [KYC AML Screening - Individuals](#)

Method: PUT

URL: <https://connect.creditsafe.com/v1/compliance/kyc-protect/searches/individuals/{searchId}/hits/{hitId}>

Required Parameters

- **PATH PARAMETERS**
 - **searchId** (required, string): The ID of the search to which the hit belongs.
 - **hitId** (required, string): The specific ID of the hit being updated.

Request Body Schema:

- **decision** (string or null): The new status of the hit. Acceptable values include:
 - **undecided**
 - **trueMatch**
 - **falsePositive**
 - **discarded.**
- **note** (string or null): Optional free text to provide context or justification for the decision.

This operation allows for precise adjustments to search hits, ensuring that each is accurately categorized based on the latest available information.

Batch Update

For situations requiring updates to multiple hits within the same search, the Batch Update process streamlines this operation by allowing you to submit changes for several hits simultaneously.

Endpoint

Tag: [KYC AML Screening - Individuals](#)
Method: PUT
URL: <https://connect.creditsafe.com/v1/compliance/kyc-protect/searches/individuals/{searchId}/hits>

Required Parameters

- PATH PARAMETERS

- **searchId** (required, string): The ID of the search whose hits are being updated.

Request Body Schema:

items (Array of objects): Each object in the array represents a hit to be updated, containing the following fields:

- **decision** (string or null): The new status of the hit (undecided, trueMatch, falsePositive, discarded).
- **note** (string or null): Optional free text for additional context or justification.
- **hitId** (string or null): The ID of the hit being updated.

Batch updates facilitate the efficient management of search results, enabling you to swiftly categorize multiple hits according to their relevance or accuracy.

Return Full Search Hit Information

Introduction

Delving deeper into the AML Screening process, this endpoint is designed to retrieve comprehensive details about a specific search hit. Accessing this full information provides a granular view of the hit, encompassing:

- Business Links: Connections related to the business entity in question.
- Individual Links: Connections pertaining to individual entities.
- AML Results: Detailed Anti-Money Laundering findings, including the sources from which this information was derived.

Important Note:

Upon calling this endpoint, the returned information is recorded in the database as a permanent snapshot, capturing the details at that specific moment. This feature marks a critical distinction from merely accessing summary data, offering a deeper layer of insight and permanence regarding the hit's information.

Endpoint

Categorized under KYC AML Screening – Individuals, this endpoint facilitates an in-depth review of individual search hits.

Tag: [KYC AML Screening – Individuals](#)

Method: GET

URL: <https://connect.creditsafe.com/v1/compliance/kyc-protect/searches/individuals/{searchId}/hits/{hitId}>

Required Parameters

- **PATH PARAMETERS**

- **searchId:** The unique identifier of the search.
- **hitId:** The unique identifier of the specific hit being investigated.

This endpoint necessitates precise identification of both the 'searchId' and 'hitId' from previous interactions, ensuring the targeted retrieval of detailed information about a search hit. The requirement for these identifiers underscores the importance of accurate record-keeping and tracking within the AML Screening workflow.

Utilizing this endpoint significantly enhances the understanding of search hits, providing stakeholders with detailed insights necessary for informed decision-making and compliance management. It represents an

essential tool in the comprehensive assessment of AML Screening results, contributing to the robustness of your compliance efforts.

AML Screening - Business Searches

Introduction

AML Screening for businesses is an essential part of our compliance services, aimed at conducting thorough investigations into business entities. This structured search process is divided into three primary sections, with an additional optional endpoint available for a more in-depth analysis.

Core Sections of Business AML Screening:

- **Perform the Search for a Business:** Begin the screening process by conducting a detailed search to identify potential matches or risk factors associated with a business entity. [\[Detailed Description HERE\]](#)
- **Return the Search Hits for the Search:** Upon completion of the search, examine the hits or matches identified to analyse their relevance and potential impact. [\[Detailed Description HERE\]](#)
- **Update the Hits to Determine Status:** Evaluate each hit to categorize the nature of the match. Possible outcomes include:
 - **True Match:** Confirmation that the hit accurately identifies the business entity.
 - **False Positive:** Determination that the hit is mistakenly associated with the business.
 - **Undecided:** Instances where it is not possible to make a definitive judgment.
 - **Discarded:** Hits deemed irrelevant or incorrect, and therefore disregarded. [\[Detailed Description HERE\]](#)

Note: These can either be updated in batch or individually.

Optional Endpoint:

- **Return Full Details on a Specific Search Hit:** This optional endpoint facilitates the retrieval of comprehensive details about a particular match, offering deeper insights for cases that warrant further investigation. [\[Detailed Description HERE\]](#)

The AML Screening process is intricately linked with the profiles created within our system, underscoring the importance of the accurate and meaningful naming of profiles. While searches can be conducted independently of profiles, it's crucial to understand that monitoring capabilities are contingent upon linking a search to a specific profile. This linkage ensures that the search and its outcomes are directly associated with the correct

entity profile, facilitating a streamlined compliance and verification workflow. Conducting searches within the context of a profile not only enhances the relevancy of the search results but is also a prerequisite for activating ongoing monitoring services. Therefore, to leverage the full spectrum of our AML Screening functionalities, including continuous monitoring, linking searches to profiles is essential.

Search For A Business

Introduction

Conducting a business search within our KYC AML Screening framework is streamlined to ensure precise and relevant results. To initiate a search, three essential parameters must be provided:

Endpoint

This operation is categorized under the KYC AML Screening – Businesses tag in our online integration documentation for easy reference.

Tag: [KYC AML Screening – Businesses](#)

Method: POST

URL: <https://connect.creditsafe.com/v1/compliance/kyc-protect/searches/businesses>

Example Request Body:

```
{
  "threshold": 85,
  "name": "Creditsafe ",
  "datasets": [
    "INS"
  ]
}
```

The 'Tag in our online documentation serves as a navigational aid, guiding you to the relevant section for detailed information about using this specific endpoint.

Required Parameters

Name: The legal or registered name of the business you are searching for. It is crucial that this name matches the business's official registration to ensure accurate search results.

Threshold: An integer value that sets the minimum confidence score for search results. Valid options include: 75, 80, 85, 90, 95, 100. Only search results that meet or exceed this threshold will be returned, allowing you to filter results based on their relevance and accuracy.

Datasets: Specifies the type of data you wish to include in your search. Depending on the nature of your compliance checks, you may require information from one or more of the following datasets:

AM - Adverse Media

ENF - Enforcement

INS - Insolvency

PEP - Politically Exposed Persons (All)

PEP-LINKED - Only linked PEPs (PEP by Association)

POI - Profile of Interest

SAN - Sanctioned (All)

SAN-CURRENT - Only current Sanctions

SAN-FORMER - Only former Sanctions

SOE - State Owned Enterprises (All)

SOE-CURRENT - Only current SOE

SOE-FORMER - Only former SOE

To include multiple datasets in your search, list the three-letter codes in an array within the request body.

By adhering to these guidelines and utilizing the specified parameters, you can effectively perform targeted business searches that align with your compliance and risk management objectives.

Return Business Search Hits

Introduction

Once a business search is initiated, retrieving the detailed results is facilitated through the subsequent endpoint, which requires incorporating the searchId obtained from the initial search summary.

Understanding the Results:

- **Result Presentation:** When the search identifies more than one potential business match, the results are presented in an array, each detailed with a hitScore. This scoring quantifies the relevance of each match to the search criteria.
- **Identification of Hits:** Each result within the array is assigned a unique hitID, essential for the next step of assessing and updating the relevance of each hit. Distinguishing between the searchId and the hitID is crucial for accurately managing the search outcomes.

Categorizing Search Hits: Evaluate each business search hit and categorize it based on its relevance:

- **True Match:** The hit accurately corresponds to the business entity being searched.
- **False Positive:** The hit is mistakenly associated with the business entity.
- **Undecided:** The relevance of the hit to the business entity is unclear.
- **Discarded:** The hit is deemed irrelevant to the search criteria and is thus disregarded.

The summary information provided should offer enough insight to make an informed decision regarding the business entity's relevance of interest.

Important Consideration:

- In cases where the evaluation of a hit results in an "Undecided" or "True Match" status, it is recommended to link this outcome to the respective business profile post-status update. This step ensures that search results with potential relevance or confirmed accuracy are systematically recorded within their profiles. The differentiation between 'searchId and 'hitID becomes increasingly important as the process advances, emphasizing the need for precision in managing these identifiers.

Note: At this stage, no summary information is stored in the database, serving purely for review and decision-making purposes.

Proceeding with Hit Updates:

Updating the relevance status of business search hits necessitates the use of the designated endpoint for hit evaluation.

Endpoint

Listed under KYC AML Screening – Businesses within our online integration documentation, simplifying access and reference.

Tag: [KYC AML Screening - Businesses](#)

Method: GET

URL: <https://connect.creditsafe.com/v1/compliance/kyc-protect/searches/businesses/{searchId}/hits>

Leveraging this endpoint allows for an in-depth review of business search hits, enabling informed decisions on their relevance and facilitating the precise updating of their status. This critical step refines the search results, ensuring subsequent actions and profile linkages are grounded in accurate and pertinent information, thereby enhancing the effectiveness of the compliance framework.

Update Search Hits

Introduction

There are two methods to update search hits, in the even that only one search hit needs to be updated there is an endpoint that will specifically deal with a single case.

In the even that more than once hit is returned the 'batch update' can be used. Since all hits needs to be dealt with, it is most likely that this endpoint will be used.

Single Hit Update

Updating the status of a single search hit is essential, as each hit identified during the AML Screening process necessitates a definitive action. This operation allows you to accurately categorize the relevance or accuracy of an individual hit.

Endpoint

Tag: [KYC AML Screening - Businesses](#)

Method: PUT

URL: <https://connect.creditsafe.com/v1/compliance/kyc-protect/searches/businesses/{searchId}/hits/{hitId}>

Required Parameters:

- **PATH PARAMETERS**
 - **searchId** (required, string): The ID of the search to which the hit belongs.
 - **hitId** (required, string): The specific ID of the hit being updated.

Request Body Schema:

- **decision** (string or null): The new status of the hit. Acceptable values include:
 - **undecided**
 - **trueMatch**
 - **falsePositive**
 - **discarded.**
- **note** (string or null): Optional free text to provide context or justification for the decision.

This operation allows for precise adjustments to search hits, ensuring that each is accurately categorized based on the latest available information.

Batch Update

For situations requiring updates to multiple hits within the same search, the Batch Update process streamlines this operation by allowing you to submit changes for several hits simultaneously.

Endpoint

Tag: [KYC AML Screening - Businesses](#)

Method: PUT

URL: <https://connect.creditsafe.com/v1/compliance/kyc-protect/searches/businesses/{searchId}/hits>

Required Parameters

- **PATH PARAMETERS**

- **searchId** (required, string): The ID of the search whose hits are being updated.

Request Body Schema:

items (Array of objects): Each object in the array represents a hit to be updated, containing the following fields:

- **decision** (string or null): The new status of the hit (undecided, trueMatch, falsePositive, discarded).
- **note** (string or null): Optional free text for additional context or justification.
- **hitId** (string or null): The ID of the hit being updated.

Batch updates facilitate the efficient management of search results, enabling you to swiftly categorize multiple hits according to their relevance or accuracy.

Return Full Search Hit Information

Introduction

Access comprehensive details on a business search hit through this endpoint, which delivers an in-depth look into various aspects of a business entity. This includes business affiliations, AML results, and the origins of the collected data.

Important Note:

The act of retrieving information via this endpoint automatically stores it as a snapshot in the database, representing a fixed record of the data at the moment of access. This feature sets it apart from summary data requests, highlighting the endpoint's role in providing detailed insights and storing this information for future reference.

Endpoint

This functionality falls under KYC AML Screening – Businesses, facilitating direct access to detailed business search hit information.

Tag: [KYC AML Screening – Businesses](#)

Method: GET

URL: <https://connect.creditsafe.com/v1/compliance/kyc-protect/searches/businesses/{searchId}/hits/{hitId}>

Required Parameters

- **PATH PARAMETERS**

- **searchId:** Identifies the search from which the hit originates.
- **hitId:** Specifies the individual hit being examined.

Employing this endpoint allows for a thorough examination of business-related search hits, ensuring a comprehensive understanding and documentation of each identified risk or connection.

Adding A Search to a Profile

Introduction

Incorporating a search into a profile effectively links all associated hits to that profile. This action is critical for maintaining a coherent and relevant record of searches conducted on an entity.

To ensure accuracy and relevance, it is vital to utilize the Update Search Hits endpoint beforehand to confirm that only pertinent hits—those marked as **trueMatch** or **undecided**—are included.

Important Consideration:

Utilizing the monitoring functionality hinges on this process. Adding a search to a profile is a necessary precursor to activating monitoring services, ensuring that ongoing surveillance is both relevant and accurate.

Endpoint

This operation is classified under KYC Individual Profile Management, reflecting its role in enhancing and refining the individual profile management process.

Tag: [KYC Individual Profile Management](#)

Method: POST

URL: <https://connect.creditsafe.com/v1/compliance/kyc-protect/profiles/{profileId}/searches/link>

Required Parameters:

- PATH PARAMETERS
 - profileId: The unique identifier of the profile to which the search(es) will be added.

Example Usage

```
{
  "searchIds": [
    "497f6eca-6276-4993-bfeb-53cbbbba6f08"
  ]
}
```

Batch Addition

The system accommodates the addition of multiple searches in a single request. The server's response will delineate between successfully linked searches and any that failed to be added, providing clear feedback for each item processed.

By carefully managing which searches are added to a profile, entities can ensure that their profiles are comprehensive and accurately reflect the conducted AML screenings.

This step is not only about record-keeping but also about setting the groundwork for effective, ongoing compliance monitoring.

Adding Search To Monitoring

Introduction

Adding searches to monitoring is a pivotal step for continuous vigilance over AML and KYC compliance activities. This feature schedules specified searches for ongoing monitoring, ensuring timely updates and actions on any new or changing information.

Prerequisite:

It is a prerequisite that the search must first be added to a profile. Without this crucial step, the option to add a search to monitoring will not be available. This requirement ensures that only relevant and structured searches are incorporated into the monitoring schedule, aligning with specific profile criteria and objectives.

Endpoint

The inclusion in KYC Monitoring Management signifies this operation's pivotal role in streamlining the monitoring process, enhancing the management and tracking of individual profiles subjected to KYC compliance checks.

Tag: KYC Monitoring Management

Method: POST

URL: <https://connect.creditsafe.com/v1/compliance/kyc-protect/schedules>

Required Properties

Request Body Schema:

items: An array of objects

threshold: Defines the threshold for the schedule, with permissible values of 75, 80, 85, 90, 95, 100.

Altering the threshold may necessitate reevaluation of previously decided results.

datasets (Array of strings): Specifies which datasets to apply during the schedule's execution. Changing datasets can lead to the reassessment of previously decided results.

isEmailRequired (boolean): Indicates whether an email notification should be dispatched post-schedule execution. This is conditional upon the specification of email recipients.

emailRecipients (Array of strings or null): Enumerates the email addresses designated to receive notifications after each execution. Notifications are contingent on isEmailRequired being true.

searchId (string, <uuid>): The unique identifier of the search intended for monitoring.

Additional Information

Credits Deduction:

Utilizing different thresholds and datasets triggers the generation of new results, potentially revisiting existing hits for further decisions.

In such cases, two credits are deducted—one for monitoring and another for screening. Conversely, if thresholds and datasets remain unchanged, only one credit is deducted for the monitoring process.

This operation not only facilitates the seamless inclusion of searches into the monitoring mechanism but also underscores the necessity for meticulous management of compliance endeavours. By leveraging this feature, organizations can ensure that their monitoring strategies are both comprehensive and aligned with the latest compliance standards, thereby mitigating potential risks effectively.

Update Monitoring Schedules

Introduction

Monitoring schedules are essential for keeping your KYC processes up-to-date and efficient. There are two primary methods for updating schedules: updating multiple schedules simultaneously and updating a single schedule by its unique scheduleId. Both methods utilize PUT calls and require specific information in the requestBody.

Important Notes:

Data and Threshold Changes: Adjusting the threshold or datasets can generate new results, potentially revisiting existing hits for further review. Such changes necessitate decisions on newly returned hits.

Credit Deduction:

Altering the threshold or datasets will result in the deduction of one credit for screening. For details on datasets, refer to Appendix E.

Update Multiple Schedules

Endpoint

Tag: KYC Monitoring Management

Method: PUT

URL: <https://connect.creditsafe.com/v1/compliance/kyc-protect/schedules>

RequestBody Requirements

To update multiple schedules, submit an array of items within the request body, each containing:

Required Properties:

threshold: The sensitivity threshold for the schedule.

datasets: An array specifying which datasets to apply.

scheduleId: The unique identifier for each schedule to be updated.

Optional Properties:

isEmailRequired: Boolean indicating if an email notification is needed.

emailRecipients: An array of email addresses to receive notifications.

Example

```
{
  "items": [
    {
      "threshold": 80,
      "datasets": [
        "string"
      ],
      "isEmailRequired": true,
      "emailRecipients": [
        "string"
      ],
      "scheduleId": "3fa85f64-5717-4562-b3fc-2c963f66afa6"
    }
    {
      "threshold": 0,
      "datasets": [
        "string"
      ],
      "isEmailRequired": true,
      "emailRecipients": [
        "string"
      ],
      "scheduleId": "3fa85f64-5717-4562-b3fc-2c963f66afa7"
    }
  ]
}
```


Update a Single Schedule

Endpoint

Tag: KYC Monitoring Management

Method: PUT

URL: <https://connect.creditsafe.com/v1/compliance/kyc-protect/schedules/{scheduleId}>

To update a single schedule, include the `scheduleId` in the URL path and specify the following properties in the request body:

Required Properties

threshold: The sensitivity threshold for the schedule.

datasets: An array specifying which datasets to apply.

Optional Properties:

isEmailRequired: Boolean indicating if an email notification is needed.

emailRecipients: An array of email addresses to receive notifications.

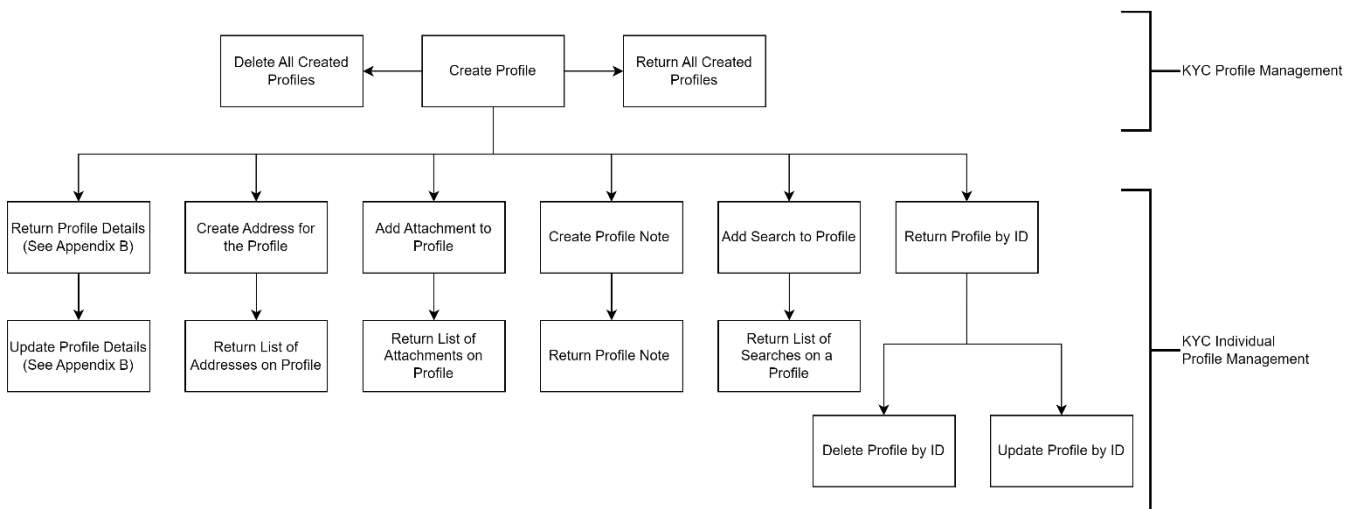
Example

```
{
  "threshold": 80,
  "datasets": [
    "string"
  ],
  "isEmailRequired": true,
  "emailRecipients": [
    "string"
  ],
}
```

Appendices

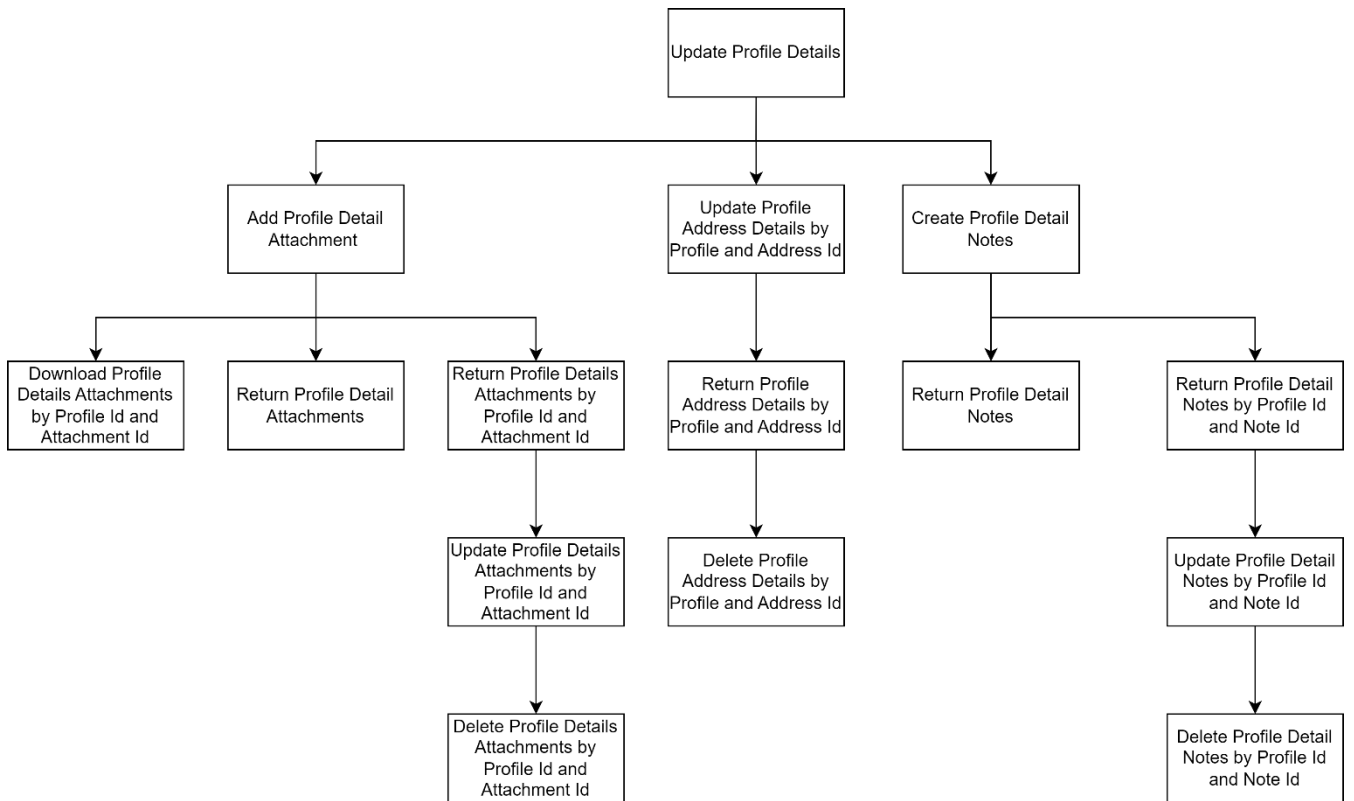
Appendix A

Additional Endpoints Post Profile Creation



Appendix B

Additional Endpoints at Profile Detail Level



Appendix C

Additional Endpoints post Individual / Business Search

Appendix D

Additional Endpoints at Search Hits Level

Appendix E

Individual and Business Dataset Tables

DATASETS			
INDIVIDUAL		BUSINESSES	
ENUM VALUE	DESCRIPTION	ENUM VALUE	DESCRIPTION
AM	Adverse Media	AM	Adverse Media
DD	Disqualified Director	INS	Insolvency
INS	Insolvency	PEP	Politically Exposed Persons
PEP	Politically Exposed Persons	PEP-LINKED	Only Linked PEPS (By Association)
PEP-CURRENT	Only Current PEPS	POI	Profile of Interest
PEP-FORMER	Only Former PEPS	ENF	Enforcement
PEP-LINKED	Only Linked PEPS (By Association)	SAN	Sanctioned
POI	Profile of Interest	SAN-CURRENT	Only Current Sanctions
ENF	Enforcement	SAN-FORMER	Only Former Sanctions
SAN	Sanctioned	SOE	State Owned Enterprises (All)
SAN-CURRENT	Only Current Sanctions	SOE-CURRENT	Only Current SOE
SAN-FORMER	Only Former Sanctions	SOE-FORMER	Only Former SOE